European Union Claims of Jurisdiction over the Internet

An Analysis of Three Recent Key Developments

by **Dan Jerker B. Svantesson***

Abstract: The topic of Internet jurisdiction is gaining a considerable amount of attention at the moment. Yet, we are seemingly still a long way from solutions. This article builds on the notion that we are presently in an era of jurisdictional "hyper-regulation" characterised by complexity and a real risk of Internet users being exposed to laws in relation to which they have no realistic means of ensuring compliance. Drawing upon a framework consisting of three jurisdictional core principles, the article seeks to examine whether three recent key developments in EU law contribute to hyper-regulation. Those three developments are: (1) Article 3 of the General Data Protection Regulation (GDPR) which outlines the Regulations "territorial scope"; (2) The combined effect of the proposed e-evidence Directive and the proposed e-evidence Regulation; and (3) the Court of Justice of the European Union (CJEU) decision in Bolagsupplysningen OÜ. The article also provides an analysis of recent trends and draws some conclusions as to how we may best move forward in this field.

Keywords: Internet jurisdiction; GDPR; hyper-regulation; law enforcement; CJEU; scope of jurisdiction; e-evidence; substantial connection; legitimate interest; interest balancing

Recommended citation: Dan Jerker B. Svantesson, European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments, 9 (2018) JIPITEC 113 para 1.

A. Introduction

1 When we engage in activities online, we are bound by law. While this may have been a controversial claim in the mid-90s, it is today little more than a truism. But the details of this truism remain contentious; that is, while it is clear that we typically must abide by the laws of the state in which we are located when engaging in the relevant online activity, to what extent do we also – at the same time – need to abide by other states' laws? This is by no means a novel issue. I have myself written about it for almost 20 years, others have considered this matter for an even longer time,[1] and there are numerous interesting, new approaches being advocated.[2] Despite the frustratingly many hours people have devoted to thinking about and debating this matter, it remains a "live" issue today.

2 To understand the complications involved, we must first realize that the number of laws a person is expected to comply with when engaging in online

* Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden).

1 Consider, for example, the important works of Johnson and Post, "Law and Borders - The Rise of Law in Cyberspace", 48 Stan. L. Rev. (1996), 1367; Reidenberg, "Lex Informatica", 76(3) Tx. L. Rev. (1998), 553; Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 Mich. Telecom. & Tech. L. Rev. (1998), 69; Goldsmith, "Against Cyberanarchy", 65 U. Chicago L. Rev. (1998), 1250; Geist, "Is There a There There? Towards Greater Certainty for Internet Jurisdiction", 16 Berkeley Tech. L.J. (2001), 1345.

2 See, e.g., Lutzi, "Internet Cases in EU Private International Law— Developing a Coherent Approach", 66 ICLQ (July 2017), 687–721, and Taylor, "Transatlantic Jurisdictional Conflicts in Data Protection Law" (forthcoming).

activities is not static. Rather it varies depending on a range of factors and must be approached as something context-specific. In other words, the number of laws, and which laws, a person is expected to comply with when engaging in one online activity (e.g. sending an email from Sweden to Luxembourg, discussing the activities of a person in Russia) will be markedly different to the number of laws, and which laws, the same person is expected to comply with when engaging in another online activity (e.g. posting information about Chinese officials on a US social media site on which the person making the posting has "friends" in 50 different countries). Thus, for any specific activity, we can speak of a "contextual legal system" consisting of the norms of all those states' laws that the person in question is expected to abide by in relation to the given activity.[3]

3 It may, however, be quite impossible for a person to ascertain all the norms of the contextual legal system by which she is expected to abide. The obvious obstacles include problems accessing the relevant law, language barriers and legal uncertainties, as well as the practical issue of identifying which states' laws make claim to be part of the relevant contextual legal system in the first place. In fact, predictability here requires nothing less than a complete knowledge of all the laws of all the states in the world, including their respective private international law rules on jurisdiction, choice of law, declining jurisdiction, as well as on recognition and enforcement.

4 Furthermore, given that each such contextual legal system is made up of norms from multiple states' legal systems – norms that typically are neither coordinated, nor harmonized, with the norms of the other states' legal systems – it will surprise no one that the contextual legal system to which a person is exposed may contain clashing norms; that is, the norms of one state may order something that the norms of another state forbids, or the norms of one state may outline duties that directly contradict rights provided for under the norms of another state.

5 The situation I have just described may be referred to as a form of "hyper-regulation",[4] and it involves the following conditions: (1) the complexity of a party's contextual legal system amounts to an unsurmountable obstacle to legal compliance; and (2) the risk of legal enforcement of—at least parts of—the laws that make up the contextual legal system is more than a theoretical possibility.[5]

6 This article seeks to examine three recent key developments in European Union law and to assess the extent to which they contribute to hyper-regulation as defined above. More specifically, attention will be directed at the impact of:

- Article 3 of the General Data Protection Regulation (GDPR) which outlines the Regulation's "territorial scope";
- The combined effect of the Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (hereinafter "proposed e-evidence Directive"),[6] and the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (hereinafter "proposed e-evidence Regulation");[7] and
- The Court of Justice of the European Union (CJEU) decision in *Bolagsupplysningen OÜ*.

7 In examining these three developments, account will be taken of what traditionally is discussed as personal jurisdiction (i.e. jurisdiction over the relevant party), as well as what may be referred to as "scope of jurisdiction", or "scope of (remedial) jurisdiction". Scope of jurisdiction relates to the appropriate geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction.[8] This question has gained far less attention to date than other jurisdictional issues. Yet, while this third dimension is often overlooked, it is doubtless a major arena for hyper-regulation.

8 Finally, by way of introduction, the analysis of the extent to which the examined developments in European Union law contribute to hyper-regulation will be assisted by a jurisprudential framework I have presented elsewhere[9] that outlines three core

3 See, further, Svantesson, "The holy trinity of legal fictions undermining the application of law to the global Internet", 23(3) Int'l J. of L. and Info. Tech. (2015), 219-234.

4 See, further, Svantesson, *Solving the Internet Jurisdiction Puzzle*, (OUP, 2017), pp. 105-111.

5 See, further, Svantesson, *Are we stuck in an era of jurisdictional hyper-regulation?*, (Institutet för rättsinformatik, forthcoming 2018).

6 Strasbourg, 17.4.2018, COM(2018) 226 final, 2018/0107(COD), Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

7 Strasbourg, 17.4.2018, COM(2018) 225 final, 2018/0108(COD), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

8 See, further, Svantesson, "Jurisdiction in 3D – 'scope of (remedial) jurisdiction' as a third dimension of jurisdiction", 12(1) J. Private Int'l L. (2016), 60-76.

9 Svantesson, "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft", 109 Am. J. of Int'l L. Unbound 69 (2015), <https://www.cambridge.org/core/journals/american-journal-

principles that, in my view, guide jurisdictional claims. Under that framework:

> In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:
>
> (1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction;
>
> (2) the State seeking to exercise jurisdiction has a legitimate interest in the matter; and
>
> (3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests.

9 While this framework was developed to illustrate the true jurisprudential core principles that underpin jurisdiction (in both public, and private, international law), the three principles can also serve the function of a diagnostics tool that may identify the cause of *why* a certain jurisdictional claim goes too far so as to contribute towards hyper-regulation. I hasten to acknowledge that I recognize the somewhat schizophrenic use to which I put this framework. On the one hand, I claim that it describes the true jurisprudential core principles underpinning jurisdiction. This implies that all jurisdictional claims are anchored in these principles. But on the other hand, I am suggesting that the framework can be used to assess specific jurisdictional claims, which implies that not all jurisdictional claims are anchored in these principles. This may, however, not be quite the contradiction it appears to be at a first glance.

10 The fact that a particular phenomenon is anchored in a certain way of thinking obviously does not prevent occurrences straying from the mentioned thinking. And where the situation is such that more occurrences are straying from the thinking that was previously dominant than not, we may speak of a paradigm shift. Thus, my claim may be best expressed in the following. As I see it, under our current paradigm (which I argue has moved away from territoriality as the core of jurisdiction),[10] legitimate jurisdictional claims are founded in the principles I have outlined in my framework. Thus, this framework both describes the true jurisprudential core principles underpinning jurisdiction and allows us to use this framework to assess whether specific jurisdictional claims have strayed from these core principles.

11 At any rate, before starting the analysis alluded to, we first need to consider the general safeguards contained in EU law imposing restrictions on jurisdictional claims that may otherwise contribute to the trend of hyper-regulation.

B. General safeguards

12 The fact that US law imposes restrictions on jurisdictional claims is generally well-known. The reason this is so may be attributed to the fact that legal tools such as the "presumption against extraterritoriality"[11] and the "*Charming Betsy*" doctrine[12] are debated in the courts, and in academic literature, on a regular basis. In contrast, comparatively little attention has been directed at the extent to which EU law contains similar tools for limiting jurisdictional claims.

13 However, thanks to an *amicus brief* filed by the European Commission in the controversial *Microsoft Warrant* case – heard in the Supreme Court of the United States on 27 February 2018 – we now know that EU law does in fact embody similar principles to the US presumption against extraterritoriality and the *Charming Betsy* canon.[13] The Commission made the point that:

> *[a]ny domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner*

of-international-law/article/new-jurisprudential-framework-for-jurisdiction-beyond-the-harvard-draft/BA4AE9C46D9783ADC433C0C79B7B7E04> (last visited 28 May 2018).

10 If territoriality ever was the true jurisprudential core principle underpinning jurisdiction – and I doubt it ever should have been viewed as having that status – we can no longer treat the plentiful occurrences (online and offline) that stray from the territoriality-focus as mere exceptions.

11 "Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2100 (2016); *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013); *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010).

12 "Under the Charming Betsy canon, first enumerated by Chief Justice Marshall in Murray v. The Schooner Charming Betsy, U.S. courts are constrained to avoid interpreting 'an act of congress' in a manner that would 'violate the law of nations, if any other possible construction remains,' 6 U.S. (2 Cranch) 64, 118 (1804)—whether the statute at issue is meant to apply extraterritorially or not." Brief of International and Extraterritorial Law Scholars as Amici Curiae in Support of Respondent, <https://www.supremecourt.gov/DocketPDF/17/17-2/28256/20180118132126676_17-2%20bsac%20International%20and%20Extraterritorial%20Law%20Scholars--PDFA.pdf> (last visited 28 May 2018), at 3.

13 Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, p. 7, <https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf> (last visited 28 May 2018).

that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.[14]

14 In doing so, the Commission pointed to four different authorities. The first was *Treaty on European Union* (TEU) article 3(5) which reads as follows:

In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter.

15 The second was TEU article 21(1) which makes clear that:

[t]he Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law.

16 The third was Case 52/69, *Geigy v. Commission*.[15] In this matter, the Court had to address a situation involving anti-competitive conduct within the EU but orchestrated from outside the EU.

17 The fourth and final authority the Commission referred to was Case C-366/10, *Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change*,[16] which made clear that: "the European Union is to contribute to the strict observance and the development of international law. Consequently, when it adopts an act, it is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union".[17]

18 All the recent developments in EU law discussed below ought to be read keeping in mind the principles enshrined in these foundational treaties and case law.

C. Article 3 of the General Data Protection Regulation

19 There has been considerable hype around the GDPR which came into effect on 25 May 2018. It has been celebrated, and it has been feared. It has been seen as going too far, and it has been seen as not going far enough. Perhaps it is a rather safe bet to predict that the true impact will fall somewhere between these extremes.

20 In any case, Article 3, outlining the Regulation's "territorial scope", is doubtless the Regulation's most important provision for anyone outside the EU. After all, it determines whether actors outside the EU need to take account of the GDPR or whether they safely can disregard it. In other words, it is Article 3 we must turn to in order to assess whether the GDPR forms part of any given contextual legal system. This crucially important provision reads as follows:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

21 Here we may pause to consider the drafters' choice of attaching the label of "territorial scope" to Article 3. After all, if we briefly accept the conventional distinction between "territorial" and "extraterritorial", two of the three sub-sections are clearly dealing with what may be labelled the GDPR's

14 Ibid.

15 11, ECLI:EU:C:1972:73.

16 123, ECLI:EU:C:2011:864.

17 Case C-366/10, *Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change*, para 101. See further Jääskinen and Ward, "The External Reach of EU Private Law in the Light of *L'Oréal versus eBay and Google and Google Spain*", in Cremona and Micklitz, *Private Law in the External Relations of the EU*, (OUP, 2016), pp. 125-146, at 131-132.

"extraterritorial scope". In fact, given that Article 3(1) points to the Regulation applying regardless of whether the processing takes place in the Union or not, we may arguably point to an "extraterritorial" dimension of all three sub-sections.

22 Surprisingly, while the Article 29 Working Party has provided guidance on numerous aspects of the GDPR, no such guidance has been provided – at the time of writing – in relation to Article 3. Thus, actors outside of the EU have had preciously little to work with when seeking to assess whether they are caught by the GDPR. However, some guidance can be found in Recitals 22-25, most significantly, Recital 23 states that:

> *In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.*

23 In addition, Recital 24 teaches us that:

> *In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.*

24 Furthermore, unlike the Recitals, the Article 29 Working Party's general factsheet aimed at helping Asia Pacific Privacy Authorities understand the basic requirements included in the GDPR specifically includes the phrase "target individuals in the EU".[18] This may be seen to place the "directing activities test" in the terminology of "targeting" more commonly used outside the EU. The same factsheet also includes the following example illustrating the practical application of Article 3: "A Japanese web shop, offering products, available online in English with payments to be made in Euros, processing multiple orders a day from individuals within the EU and shipping these products to them, should be compliant with the GDPR".[19]

25 Unfortunately, this example raises more questions than it provides answers. We may, for example, wonder whether the Japanese web shop in question would avoid the GDPR simply by only accepting payment in non-EU currencies. And what if the Japanese web shop, rather than "processing multiple orders a day from individuals within the EU", merely accepted such orders occasionally, or once a day? What are the actual thresholds that will be applied?

26 In the end, the reality is that the "targeting test", while it looks like a neat solution on paper, gives preciously little practical guidance for the businesses, lawyers and indeed judges, who are tasked with assessing whether the test has been met in a given situation.[20]

27 Nevertheless, reading Article 3 together with the explanatory remarks in the mentioned Recitals and the Article 29 Working Party's general factsheet aimed at helping Asia Pacific Privacy Authorities, it is clear that the GDPR has a considerable reach beyond the EU. This is no accident; rather it is the expression of a clearly articulated policy goal, namely that of ensuring that non-EU actors engaging on the EU market are caught by the GDPR so as to create what has been promoted as a "level playing field".[21]

---

18 "The GDPR applies to data controllers and data processors with an establishment in the EU, or with an establishment outside the EU that target individuals in the EU by offering goods and services (irrespective of whether a payment is required) or that monitor the behavior of individuals in the EU (where that behavior takes place in the EU). Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union." Article 29 Working Party, EU General Data Protection Regulation: General Information Document, p. 2, <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49751&lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3BaEuuvVHcSFSSShxXB0Rnjg%3D%3D> (last visited 28 May 2018).

19 Ibid.

20 See, further, Oster, "Rethinking Shevill. Conceptualising the EU Private International Law of Internet Torts Against Personality Rights", 26 Int'l Rev. L. Compu. & Tech. (2012), 113, at 118 and Svantesson, "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation", 5(4) Int'l Data Privacy L. (2015), 226-234.

21 See, e.g., Reding, "The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights", (Intervention at the Justice Council, Brussels, 4 Mar. 2014), <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm> (last visited 28 May 2018). A similar sentiment is expressed by Jan Philipp Albrecht in "Regaining Control and Sovereignty in the Digital Age", in Wright and De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, (Springer, 2016), pp. 473–88, at 476.

28 It is not difficult to see the political appeal of such a levelling of the playing field; after all, why should foreign businesses be given a competitive advantage by avoiding the EU's strict data protection laws when such an advantage comes at the cost of EU business and of EU consumers? The problem with this reasoning, however, is that it quite simply overlooks the fact that there is a big world outside the EU.

29 First, it overlooks the fact that countries outside the EU are used to adapting their data protection laws based on what the EU does. As a result, all EU-based businesses that may wish to engage on markets outside the EU will be more likely to have to incur the costs of ensuring compliance with multiple foreign data protection schemes. And while the EU's GDPR may be the strictest data protection regime as a whole, those who assume that compliance with the GDPR automatically ensures compliance with all other data protection schemes will soon be subject to a rude awakening.[22]

30 The second manner in which the levelling of the playing field argument fails to recognize the fact that there is a world outside the EU, relates to how foreign businesses will respond to the GDPR. The "big players" will, of course, take steps to adjust their behaviour so as to be GDPR-compliant. Indeed, they have already done so. But they are of a size and nature that means that they would have been doing so also with a much more modest, and more nuanced, claim of jurisdiction than that of GDPR Article 3. Of the small- to medium-sized businesses around the world, some may adjust their behaviour to the GDPR whether they are actually subject to it or not, but many will no doubt carry on as usual and hope they will not be subject to any enforcement actions. And given how many businesses outside the EU fall within Article 3, and taking account of the resources available for Data Protection Authorities enforcing the GDPR, perhaps the odds are in their favour. For EU citizens dealing with such businesses, it is difficult to see the GDPR bringing any improvements, and there will be no levelling of the playing field either. Furthermore, as there clearly will be more foreign businesses failing to comply with the GDPR than there are resources to investigate them, the actual application of the GDPR will necessarily be arbitrary, which arguably undermines the legitimacy of any enforcement actions taken.

31 Other small- to medium-sized businesses, and also some larger actors, around the world will simply use geo-location technologies to block users from the EU. For example, Europeans seeking to access the website of the *Chicago Tribune* (www.chicagotribune.com), are now met with the following message:

> *Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.*

32 This type of situation represents a loss for EU citizens. Proponents of Article 3 will no doubt be quick to point out that EU citizens missing out on the goods, services and contents provided by such businesses is a reasonable sacrifice for the privilege of being protected by the GDPR. This may well be true. However, it misses the point. It need not have been the case that our only choice was between foreign businesses either complying with the GDPR in its entirety, or blocking out the EU market. From a consumer perspective, some aspects of the GDPR are more important than others in their dealings with foreign businesses. For example, the EU consumer community may well have preferred not to be blocked from many foreign services as long as those services were bound to comply with the GDPR's key provisions (such as the lawfulness requirements in Article 6), even where those same services did not necessarily comply with the more administrative/bureaucratic layer of the Regulation (such as Article 37 requiring a Data Protection Officer).

33 The decision to have one single jurisdictional threshold for the entire GDPR – an instrument that seeks to achieve so many diverse objectives – is a major blunder undermining the legitimacy of the GDPR as such.[23] Rather, the drafters ought to have adopted what I elsewhere[24] have referred to as a "layered-approach" in which the relevant substantive law (here the various substantive provisions of the GDPR) is divided into different layers, with a different jurisdictional threshold for the various layers. For example, it may have been fruitful to assign provisions such as Article 6 to an "abuse-prevention layer" in relation to which a far-reaching claim of jurisdiction may be justified. Provisions such as Article 37 could fall within an "administrative layer" in relation to which the jurisdictional threshold would be high. And provisions such as Article 15 (giving a right of access by the data subject) could fall within a "rights layer" in relation to which the jurisdictional threshold would be easier to satisfy that for the administrative layer, but more difficult to satisfy that for the abuse-

22 Consider, for example, the tremendous diversity of data privacy laws described in Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, (OUP 2014).

23 Svantesson, "Extraterritoriality and targeting in EU data privacy law", op. cit. *supra* note 20, 226-234.

24 Svantesson, "A 'layered approach' to the extraterritoriality of data privacy laws", 3(4) Int'l Data Privacy L. (2013), 278-286.

prevention layer.[25]

34 The only aspect of the GDPR in relation to which it may be said that there is a jurisdictional threshold derogating from that of Article 3 is in Article 27. There it is made clear that the obligation prescribed under Article 27 – that of controller and processors caught by Article 3(2) having an obligation to designate in writing a representative in the Union – does not apply to:

> *processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;*

35 Even so, against the background of the above, the reader will not be surprised by my conclusion that GDPR Article 3 performs poorly when assessed against the framework advanced above. I would argue that while Article 3 might meet the requirements imposed by the second principle in the framework – that is, the EU has a legitimate interest in what it is pursuing – it is highly questionable whether Article 3, and especially Article 3(2), captures only those matters that have a substantial connection to the EU. Further, I most definitely do not think enough regard has been given to other relevant interests, as is required under the third principle

D. The Proposed e-evidence Directive and Regulation

36 The Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings and the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters must be read together.

37 These instruments have been advanced to address a significant issue: namely to make it easier and faster for law enforcement and judicial authorities to obtain electronic evidence often held by foreign Internet companies. Unveiled in April 2018, these proposals were preceded by a considerable period of consultations.

38 Put in the fewest of words, the combined effect of the proposed Directive and the proposed Regulation is to put in place a scheme under which service providers – including foreign service providers – are obligated to designate a legal representative in the Union. This is combined with the creation of a European Production Order and a European Preservation Order. The respective roles of the Directive and the Regulation are that, while the Directive "lays down rules on the legal representation in the Union of certain service providers for receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings",[26] the Regulation "lays down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data."[27]

39 To understand how this proposed arrangement will impact actors outside the EU, there are some key concepts that must be understood. First, the definition of the type of service providers caught by these instruments is broad and includes any natural or legal person that provides one or more of several types of services including, for example, "internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and related privacy and proxy services",[28] certain electronic communications service,[29] as well as information society services "for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers"[30].

40 To understand the jurisdictional scope, we need to start with the observation that both the Regulation and the Directive apply to service providers "offering services" in the Union or a Member State.[31] While this sounds broad, offering services in a Member State (or in the Union) means enabling legal or natural persons in a Member State to use the service and "having a substantial connection to the Member State" in question.[32] This, of course, fits neatly within the framework I have discussed above. However, an examination of the Recitals will rapidly quash any

25 See, further, ibid.

26 Proposed e-evidence Directive Art. 1(1).

27 Proposed e-evidence Regulation Art. 1(1).

28 Proposed e-evidence Directive Art. 2(2)(c) and proposed e-evidence Regulation Art. 2(3)(c).

29 Proposed e-evidence Directive Art. 2(2)(a) and proposed e-evidence Regulation Art. 2(3)(a).

30 Proposed e-evidence Directive Art. 2(2)(b) and proposed e-evidence Regulation Art. 2(3)(b).

31 Proposed e-evidence Directive Art. 1(4) and proposed e-evidence Regulation Art. 1(1).

32 Proposed e-evidence Directive Art. 2(3) and proposed e-evidence Regulation Art. 2(4).

feelings of excitement. Recital 13 of the Directive, similarly to Recital 28 of the Regulation, makes clear that a "substantial connection" does not need to be particularly substantial at all. Rather, a substantial connection to the Union exists where:

(1) the service provider has an establishment in the Union; or

(2) where the service provider does not have an establishment in the Union, but the service provider:

a. has a significant number of users in one or more Member States;

b. is targeting its activities towards one or more Member States; or

c. directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.

41 Thus, what we are really dealing with here is largely a targeting test that incorporates all the uncertainties, blemishes and warts typical of a targeting test, and which clearly has the potential to cater for far-reaching jurisdictional claims—thus, having little to do with any truly "substantial connection".

42 Further, it is interesting to note the odd double use of the targeting test, first as a stand-alone measure specifically described as targeting (2(b) in my structure above) and then targeting as articulated in the context of Article 17(1)(c) of Regulation 1215/2012 (2(c) in my structure above).[33] In the context of the former, the Recital explains that:

> *[t]he targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ("app") in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State.*

43 While there are some additional examples included (such as the reference to the relevant national app store) this is, of course, the same targeting test as that of Article 17(1)(c) of Regulation 1215/2012. Thus, this double use of "targeting" is both a sign and a potential source of confusion.

44 Against this background, the reader will already have guessed that, in my view, the approach adopted in the proposed Regulation and the proposed Directive fails to limit the jurisdictional reach of these instruments to those situations in relation to which they have a substantial connection. This is a disappointing conclusion particularly in the light of the fact that the drafters clearly were going in the right direction in that they were specifically referring to the need for a substantial connection.

45 As to the need for a legitimate interest – a term not used in the instruments – a more favourable conclusion may be reached. The drafters are clearly pursuing legitimate interests and have, for example, sought to limit the types of crimes in relation to which the measures in question may be taken.[34] Arguably some additional measures could have been taken in this context, but on the whole, the legitimate interest test may be seen to be met.

46 Finally, it is encouraging to see that a rather sophisticated interest balancing is a clearly articulated aspect of these instruments. This is particularly so in relation to Articles 15 and 16 of the Regulation. They aim to ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned, and to address conflicting obligations on service providers by providing a mechanism for judicial review in cases of clashes with legal obligation stemming from the law of third states.[35] These provisions instruct the court to engage in an interest balancing exercise:

> *weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible consequences for the service provider of having to comply with the Order.*[36]

47 Thus, the final verdict must be that, to score well under the assessment framework applied in this article, these instruments mainly need to remove the Recital's peculiar bastardization of the "substantial connection test".

33 See *Pammer v Reederei Karl Schlüter GmbH & KG* (Case C- 585/ 08) and *Hotel Alpenhof GesmbH v Oliver Heller* (Case C- 144/ 09).

34 See, e.g., Proposed e-evidence Regulation, Art. 5(4).

35 Proposed e-evidence Regulation, Recital 47.

36 Ibid., Recital 52.

E. Bolagsupplysningen OÜ

48 Claims of jurisdiction over cross-border defamation have a long history of sparking controversy. This is perhaps not surprising given that any defamation action involves the complex balancing of competing human rights, one of them being freedom of expression. And, of course, in the context of *cross-border* defamation, the balancing will, by necessity, involve the even more complex, and even more sensitive, balancing of competing human rights as viewed in different countries.

49 The EU's approach to claims of jurisdiction over cross-border defamation is articulated in what is now Article 7(2) of the *Brussels I bis Regulation*, as interpreted in three key cases. Article 7(2) reads as follows: "in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur".

50 The three key cases are *Shevill*,[37] *eDate*[38] and *Bolagsupplysningen OÜ*,[39] and it is the most recent of these – the *Bolagsupplysningen OÜ* case of October 2017 – that I am examining here. However, to understand the issues that arise from the CJEU's decision in *Bolagsupplysningen OÜ*, we must view it against its proper background which consists of *Shevill* and *eDate*.

51 *Shevill and Others*, C68/93,[40] involved an action for libel relating to a newspaper distributed in several Member States. The Court held that:

> *the victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised.*[41]

52 The *eDate* decision of 2011[42] was in fact two cases that the Court dealt with jointly. The first – *eDate Advertising GmbH v X* [43] – involved allegedly defamatory content about a German citizen having been placed on a website in Austria. The second – *Olivier Martinez, Robert Martinez v MGN Ltd* [44] – related to an infringement of personal rights allegedly committed by the placing of information and photographs on a website in another Member State. In its decision, the Court held that:

> *in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised.*[45]

53 Importantly, there are numerous indicators making clear that the Court, in both of these decisions, in speaking of "jurisdiction to award damages for all the harm caused by the defamation", is only referring to such harm occurring in Member States. For example, in *Shevill*, the only circulation discussed is that within Member States.[46] In no way did the Court suggest it was pointing to a competence as to award worldwide damages – the scope of jurisdiction is limited to the EU.

54 But let us now approach the most recent in this trilogy of key decisions. The dispute in *Bolagsupplysningen OÜ* related to proceedings brought regarding requests for the rectification of allegedly incorrect information published on a website, the deletion of related comments on a discussion forum on that website, and compensation for harm allegedly suffered. The CJEU held that:

> *a legal person claiming that its personality rights have been infringed by the publication of incorrect information concerning it on the internet and by a failure to remove comments relating to that person can bring an action for rectification of that information, removal of those comments and compensation in respect of all the damage sustained*

37 *Shevill and Others*, C68/93, EU:C:1995:61.

38 Cases C-509/09 *eDate Advertising GmbH v. X* and C-161/10 *Olivier Martinez and Robert Martinez v. MGN Limited*.

39 Case C194/16 *Bolagsupplysningen OÜ Ingrid Ilsjan v. Svensk Handel AB*.

40 EU:C:1995:61.

41 *Shevill and Others*, C68/93, EU:C:1995:61.

42 Cases C-509/09 *eDate Advertising GmbH v. X* and C-161/10 *Olivier Martinez and Robert Martinez v. MGN Limited*.

43 Case C-509/09 (Referring court Bundesgerichtshof, Germany), ECLI:EU:C:2011:685, [2011] ECR I-10269.

44 Case C-161/10 (Referring court Tribunal de grande instance de Paris, France), ECLI:EU:C:2010:685, [2011] ECR I-10269.

45 Cases C-509/09 *eDate Advertising GmbH v. X* and C-161/10 *Olivier Martinez and Robert Martinez v. MGN Limited*, para 69.

46 *Shevill and Others*, C68/93, EU:C:1995:61, para 8: "On 17 October 1989 they issued a writ in the High Court of England and Wales claiming damages for libel from Presse Alliance SA in respect of the copies of France-Soir distributed in France and the other European countries including those sold in England and Wales."

before the courts of the Member State in which its centre of interests is located.[47]

55 This conclusion must be read in the light of the CJEU's reasoning that:

> *in the light of the ubiquitous nature of the information and content placed online on a website and the fact that the scope of their distribution is, in principle, universal (see, to that effect, judgment of 25 October 2011, eDate Advertising and Others, C509/09 and C161/10, EU:C:2011:685, paragraph 46), an application for the rectification of the former and the removal of the latter is a single and indivisible application and can, consequently, only be made before a court with jurisdiction to rule on the entirety of an application for compensation for damage pursuant to the case-law resulting from the judgments of 7 March 1995, Shevill and Others (C68/93, EU:C:1995:61, paragraphs 25, 26 and 32), and of 25 October 2011, eDate Advertising and Others (C509/09 and C161/10, EU:C:2011:685, paragraphs 42 and 48), and not before a court that does not have jurisdiction to do so.*[48]

56 The limitation to the EU that was so clear in the *Shevill-eDate* case-law can perhaps be inferred here. After all, the CJEU does not expressly claim a worldwide scope of jurisdiction, and indeed, there is absolutely no discussion whatsoever about the serious consequences the CJEU's decision would have if it is meant to extend beyond the EU. At the same time, however, by emphasizing that an application for the rectification and/or removal of information online is "a single and indivisible application", the CJEU seems to be consciously going far beyond the *Shevill-eDate* case-law: from a focus on EU-wide orders to worldwide orders. This is highly problematic. It either means that the CJEU in *Bolagsupplysningen OÜ* perhaps expanded the reach of Article 7(2) of the *Brussels I bis Regulation* in a dramatic manner without engaging with the considerable implications that stem from such an expansion at all, or it means that the order in *Bolagsupplysningen OÜ* – if it is merely EU-wide so as to be consistent with the *Shevill-eDate* case-law – is in fact impossible to comply with on the CJEU's reasoning that the rectification and/or removal of information online is "a single and indivisible application".

57 Given the speed with which technology develops, it is also striking that both the Court and Advocate General Bobek, in deciding a case in 2017, sought guidance in an assessment of the state of technology made in 2011. Even if it was correct at the time of *eDate* – and I am not sure that it was – that the scope of the distribution of content placed online on a website is, in principle, universal, that assessment cannot be assumed to be correct also at the time of *Bolagsupplysningen OÜ* some six years later. When assessing geo-location technology accuracy rates, it is important to be aware that they are: (i) time-specific; (ii) location-specific; and (iii) context-specific.

58 In light of how difficult it is to know for sure how *Bolagsupplysningen OÜ* should be read, assessing this development under the framework advanced above is not entirely uncomplicated. Thus, this analysis must be approached with an if/then method. If the CJEU in *Bolagsupplysningen OÜ* intended to extend the reach of EU law beyond the EU, then the claim of jurisdiction seems to fall foul of all three principles of the framework I use here.

59 However, even if the order the CJEU has in mind is restricted to the EU, there are complications stemming from the fact that EU law (namely the *Rome II Regulation*)[49] does not regulate choice of law in matters such as *Bolagsupplysningen OÜ*. Article 1(2)(g) of the *Rome II Regulation* excludes "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation" from that Regulation. This exclusion is a direct result of the considerable differences that exist in the balancing between freedom of expression and the right to reputation amongst the Member States of the European Union. Thus, the choice of law question in non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation, is left to the domestic law of the Member State that claims jurisdiction. This must clearly impact the assessment of *Bolagsupplysningen OÜ* under the principles I have advanced. At the minimum it raises issues under the third principle, as each Member State has a strong interest in its respecting balance between freedom of expression and the right of reputation being respected.

F. A broad-brush analysis of trends

60 The examination above has focused on what may be criticized as being a rather eclectic selection of recent developments. Thus, we should, of course, be careful in drawing conclusions based on the examples above. It represents nothing but a snapshot of developments from the past two years.

61 Nevertheless, I have attended enough conferences and other events, and otherwise followed and taken part in the current discussions, to say with confidence that all three of the examined developments are major developments that have sparked considerable

47 Case C194/16 *Bolagsupplysningen OÜ Ingrid Ilsjan v. Svensk Handel AB*, para 50.

48 Ibid., para 48.

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

discussion both inside, and outside, the EU. This may indeed be important enough to amount to our first conclusion: the decisions that the EU makes as to how it engages with the online environment continues to both interest, and influence, the rest of the world. Thus, the steps the EU takes have the potential to significantly impact hyper-regulation, whether in a positive or negative direction.

62 Looking at the three developments examined, I think we can reach at least some additional significant conclusions. First, it seems likely that the idea of forced "rep localization" is here to stay as the EU's weapon of choice in dealing with foreign Internet actors. Indeed, the more EU instruments that adopt this approach, the easier it is to argue for it in any given new context. For example, the fact that an obligation to designate a legal representative for service providers not established in the EU already exists in certain acts of EU law is emphasized in the Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[50]

63 Nevertheless, it is clearly a most onerous approach for all those foreign companies that otherwise would not have any physical presence in the EU, and the extent to which the EU is able to enforce this on a big scale remains to be seen. The risk of arbitrary enforcement undermining the legitimacy of the scheme is an ever-present danger, and the EU's call for rep localization is not entirely different to the much-criticized movement towards "data localization".[51] To this may be added a purely practical matter; that is, how will a small- to medium-sized foreign company recruit a party willing to be its representative in the EU? And put in the reverse, who in the EU will be willing to assume the risk of being the representative of a small- to medium-sized foreign company with a limited presence on the EU market? The attractiveness of being a representative must surely be rather limited given that the designated legal representative can be held liable for the non-compliance of the service provider.[52]

64 Furthermore, it ought to be noted that rep localization as a response to the international nature of the Internet is not scalable. The EU approach may gain some acceptance from the fact that it is sufficient to have representation in one Member State to be allowed to act in the entire Union. That may be a price many online actors are willing to pay. However, how does that translate to the rest of the world? If Afghanistan, Argentina and Australia adopt the same approach, will it be worthwhile for the Internet companies to have representatives in each of those states too? I imagine not. To this Europeans may say that how the (largely American) tech companies interact with Afghanistan, Argentina and Australia is not their problem; and they would have a point. What I am trying to emphasize, however, is merely the fact that (1) rep localization, even to the extent that it works for the EU, is not the solution for the rest of the world, and (2) one could make the claim that, given the EU's appetite for inspiring the conduct of other states,[53] it could have done more to find a globally - or partially globally - viable solution.

65 At a first glance, it may be thought that rep localization demands such as these do not really contribute to hyper-regulation; after all, the EU could have extended its laws in the same manner without the rep localization requirement. However, as the likelihood of enforcement is a factor in the definition of hyper-regulation provided above, it is clear that rep localization demands do contribute to hyper-regulation.

66 Second, it seems clear that the targeting test has also gained in status via some of these recent developments. In fact, as seen in the proposed e-evidence Regulation and the proposed e-evidence Directive, the targeting test has also managed to infiltrate and negate direct articulations of the "substantive connection" principle – the latter being nothing but the pastry on top of a beautifully decorative pie; underneath the crust, the meat and gravy is still the distinctly unpalatable targeting test. While the targeting test may – at least in theory – be applied restrictively so as to minimize hyper-regulation, the EU's approach is so vague and provides so little predictability that it rather adds to the state of hyper-regulation.[54]

50 "This is the case, for instance, in the General Data Protection Regulation (EU) 2016/679 (Article 27) and in Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (Article 18).", Proposed e-evidence Directive, at 3.

51 See, further, Cooper and Kuner, "Data Protection Law and International Dispute Resolution", 382 Recueil des cours (2017), 9–174, at 72– 76.

52 Proposed e-evidence Directive, Art. 3(8).

53 See, further, e.g. Scott, "The New EU 'Extraterritoriality'", 51 C.M.L. Rev. (2014), 1343; Scott, "Extraterritoriality and Territorial Extension in EU Law", 62 Am. J. Comp. L. (2014), 87; Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, (Springer, 2016); Cremona and Micklitz, op. cit. *supra* note 17; Mills, "Private International Law and EU External Relations: Think Local Act Global, or Think Global Act Local?", 65(3) Int'l and Comp. L.Q. (2016), 541-579, doi:10.1017/S0020589316000208; Bradford, "The Brussels Effect", 107 Northwestern U. L. Rev. (2012), 1.

54 See further Svantesson, "Extraterritoriality and targeting in EU data privacy law", op. cit. *supra* note 20, 226-234 and 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", 27(3) Computer L. & Security Rev. (June 2011), 298-304.

67 Third, the recent developments discussed here amplify the perception that the EU takes a rather schizophrenic approach to geo-location technology, managing to, on the one hand, fear its use to the degree of regulating against its use, and on the other hand, deny its legal relevance. For example, in outlining what amounts to a substantial connection, the proposed e-evidence Directive makes the point that: "provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302 [addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market] cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union."[55] At the same time, as hinted at above, the CJEU has rather consistently turned a blind eye to the impact of geo-location technologies. This is a clear illustration of the complications that stem from the EU's "ad hoc approach for addressing the legal issues generated by globalization, the Internet, and other emerging technologies" that Jääskinen and Ward alert us to in their interesting 2016 book chapter.[56] At any rate, as geo-location technology may be used to limit the risk of hyper-regulation, both the limitation of its use[57] and the practise of ignoring its legal value may substantially contribute towards hyper-regulation.

68 Finally, it also seems fair to conclude that we are at a time at which the EU seems to be leaning towards a more aggressive stance on jurisdiction over online activities. Support for such a conclusion is hinted at in the above. But further support for this conclusion can arguably be found in the observation that this is not just a description of the EU's situation, rather it is a description of the situation in many parts of the world. Many countries are starting to adopt a more aggressive stance towards jurisdiction over online activities.[58]

69 So, does that then mean that we are nearing the end of the paradigm where jurisdiction is – as I argue – founded in the three principles to which I have sought to bring attention? I think not, and to see why, we need only consider how states react to the jurisdictional claims of other states. Some readers will recall the transatlantic showdown between France and the US that took place around the turn of millennium in the context of Yahoo!'s auctioning pages.[59] A similar situation arose recently between Canada and the US. In its June 2017 decision in *Google v Equustek*,[60] the Supreme Court of Canada ordered Google to de-index, with global effect, the websites of a company which, in breach of several court orders, was selling the intellectual property of another company (Equustek Solutions Inc.) via those websites. The decision was swiftly followed by a United States District Judge granting an injunction preventing the enforcement of the Canadian judgment.[61] Such countermeasures are natural given what is at stake and they make clear that states are still not prepared to accept wide jurisdictional claims (by others).

G. Concluding remarks

70 In this article I have sought to discuss and evaluate three key developments in how the EU is seeking to delineate the external reach of its substantive law in this age characterised by extensive and frequent cross-border interactions due to the Internet. I applied one particular method but acknowledge that there are many other ways to engage with this task. And I opted to focus on the three most important recent developments, as I see it, acknowledging that there also are other developments that are relevant. The presence of subjectivity goes without saying. Nevertheless, at least on this analysis, the picture that emerges is a sombre one. While it may be said that the EU remains at the cross-roads, the indicators suggesting that the EU will opt for a path adding significantly to the troubling trend of hyper-regulation are more plentiful than those that give hope of a reversal of this development. The best way to counter this would, in my humble opinion, be to recognise the jurisprudential framework for jurisdiction that I outlined in the introduction as being incorporated in the EU's foundational treaties. This could perhaps be achieved in more than one way, and such a move could arguably be motivated along the following lines:

I. The European Union's foundational treaties and case law enshrine the principle of mutual regard to the spheres of jurisdiction of sovereign states.

II. The jurisprudential framework for jurisdiction outlined above is an articulation of how international law approaches jurisdiction.

55 Proposed e-evidence Directive, Recital 13.

56 Jääskinen and Ward, op. cit. *supra* note 17, at 146.

57 I hasten to acknowledge that where geo-location technology is used to facilitate unjustified price-discrimination, and similar harmful practices, its use may obviously be legitimately restricted.

58 Consider, e.g., *X v. Twitter Inc.* [2017] N.S.W.S.C. 1300, and *Google Inc. v. Equustek Solutions Inc.*, 2017 S.C.C. 34, to mention merely two examples.

59 *International League Against Racism & Anti-Semitism (LICRA) v. Yahoo! Inc.* (2000) County Court of Paris, as followed by responses from US courts.

60 *Google Inc. v. Equustek Solutions Inc.*, 2017 S.C.C. 34.

61 *Google LLC v. Equustek Solutions Inc.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

III. Thus, the said jurisprudential framework for jurisdiction is incorporated within the EU's foundational treaties.

IV. And as EU legislation must be interpreted in a manner that is consistent with international law, the EU does not make jurisdictional claims that go beyond that framework.

71 Under the reasoning I advanced here, it would seem legitimate for courts in the EU to adopt the jurisprudential framework for jurisdiction, described in the introduction, as the standard against which jurisdictional claims are measured, and as the underlying guiding principles for the interpretation of the EU's jurisdictional claims.

72 At any rate, the secretariat of the Internet & Jurisdiction Policy Network – the leading multistakeholder organization engaging with the tension between the cross-border nature of the internet and national jurisdictions – frequently refer to the risk of "a legal arms race" resulting from the current jurisdictional climate online.[62] And without seeming overly alarmist, I suspect that we are at the brink of what could be a most harmful set of jurisdictional confrontation, in which the potential victims include fundamental human rights, commercial effectiveness, effective and fair law enforcement, consumer protection and indeed the Internet as we know it. The war of Internet jurisdictional claims is about to begin, and in that context, I am merely seeking to be a "jurisdictional peace activist".

Acknowledgements

This article was written during two intensive weeks as a Visitor at the Court of Justice of the European Union. I am very grateful to the Cabinet of Judge Carl Gustav Fernlund for being so welcoming, and to the numerous other helpful and friendly persons I had the privilege of meeting while at the Court. All views are, of course, those of the author alone and based solely on the author's desk research carried out in the CJEU's beautiful and well-equipped library.

62 See, e.g., Internet & Jurisdiction Policy Network, "Towards Policy Coherence and Joint Action: Secretariat Summary and Ottawa Roadmap", p. 3, <https://www.internetjurisdiction.net/uploads/pdfs/Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf> (last visited 28 May 2018).