

# UNMASKING ANONYMOUS ONLINE INFRINGEMENTS OF PERSONALITY RIGHTS: QUESTIONS ARISING IN INTERNATIONAL CONTEXTS

Koji TAKAHASHI\*

- I. Introduction
- II. Stakeholders
- III. Japanese Approach
  - A. Choice of Law Question
  - B. Jurisdictional Question
- IV. French Approach
  - A. *UEJF v. Twitter*
  - B. Comments
- V. US Approach
  - A. Jurisdictional Analysis before Identification of Defendant
  - B. Where to Sue
- VI. English Approach
  - A. Personal Jurisdiction
    - 1. *Lockton Companies International v. Persons Unknown, Google*
    - 2. *Bacon v. Automattic and Others*
    - 3. Comments
  - B. Jurisdiction to Prescribe
- VII. Cross-Border Enforcement of Disclosure Orders
  - A. Necessities for Cross-Border Enforcement
  - B. Enforcement of Foreign Disclosure Orders in California
- VIII. Conclusions

## I. Introduction

When a defamatory content has been posted on a website (① in FIGURE below), the injured person may wish to seek an injunction or damages against the author<sup>1</sup>

---

\* Professor, Doshisha University Law School (Japan).

<sup>1</sup> The injured person may also demand, if possible under the applicable law, the host of the server or website on which the offending content has been published to delete it. It is, however, not always an effective remedy since the infringer often repeats posting offending contents.

(④ in FIGURE). But if the author has acted anonymously or pseudonymously,<sup>2</sup> the injured person may first need to unmask him or her by seeking orders against the internet service providers (ISPs)<sup>3</sup> demanding disclosure of the information which allows for the identification of the author. More specifically, it may be necessary to demand the content provider (the host of the server or website) to reveal the internet protocol (IP) address used to post the offending content and the time stamps of the post (② in FIGURE). With a query and response protocol called WHOIS,<sup>4</sup> the IP address allows for the identification of the internet access provider used. That provider may then be requested to check its log of IP addresses and time stamps<sup>5</sup> to ascertain the matching subscriber and to reveal his or her name (③ in FIGURE), the idea being that the subscriber is likely to be the author.<sup>6</sup>

This article will consider questions related to conflict of laws which may arise in the international dimensions of the process outlined above. They are questions of choice of law, personal jurisdiction, jurisdiction to prescribe and the cross-border enforcement of disclosure orders. What questions arise and how they arise differ depending on the precise approach taken in the process outlined above. This article will, therefore, compare and contrast the approaches taken in Japan, France, United States and England. The analysis of this article is equally applicable to the online infringement of other personality rights such as the right to privacy, portrait rights and publicity rights.<sup>7</sup>

---

<sup>2</sup> In some cases, the author impersonates the injured person and posts contents which damage the latter's reputation.

<sup>3</sup> In the present article, the word "ISPs" is used to cover both hosting service providers, *i.e.* the hosts of the server or website on which the infringing content is published, and internet access providers.

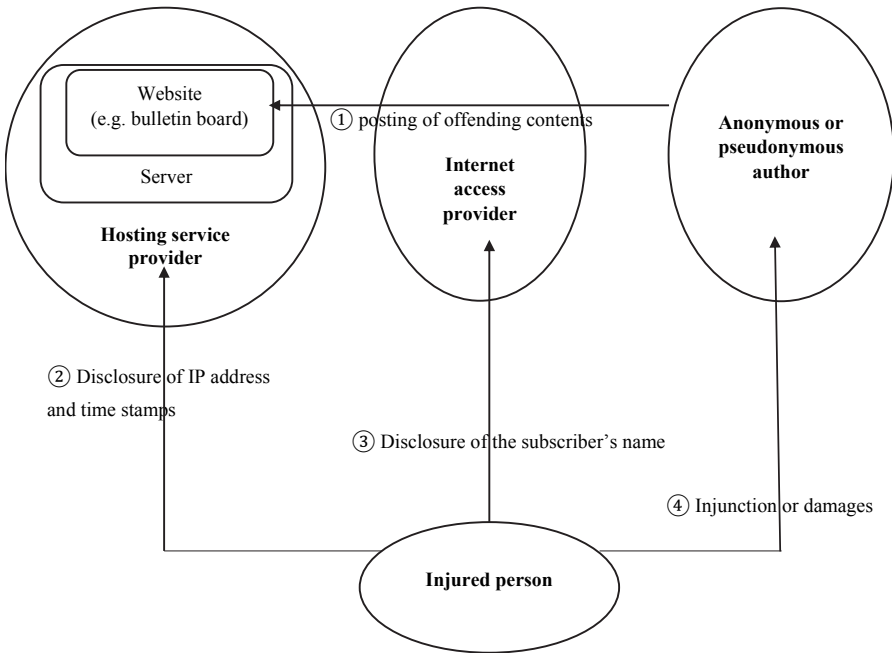
<sup>4</sup> *E.g.* <<https://who.is/>>.

<sup>5</sup> Other details may also be useful. If, for example, the author's e-mail address is registered with the hosting service provider and it has been disclosed, the injured person may request the provider of that e-mail address to reveal the name of the holder of that address.

<sup>6</sup> They are not always the same. Where, for example, the subscriber is an internet café making its internet access generally available to its customers, the café is unlikely to be the author. The subscriber may dispute that he or she is the actual author once an action for damages or injunction is brought against him or her.

<sup>7</sup> Much of the analysis is also applicable to the cases of online infringement of intellectual property rights such as illegal downloading and file sharing. Reference will, therefore, be made to such cases insofar as they are informative.

FIGURE



## II. Stakeholders

Before embarking on the comparative analysis, it is worth examining the respective interests of the stakeholders involved in the process of unmasking an anonymous online author since the consideration of questions arising in the process should take such interests into account.

The injured person obviously has interest in vindicating his or her personality rights. But the interest which matters in the context of the present analysis is that of obtaining access to justice to vindicate those rights.

The author has interest in anonymously exercising his or her right to freedom of expression.<sup>8</sup> Once his or her identity has been revealed, the unmasked

---

<sup>8</sup> To protect this interest, each legal system sets a substantive threshold for obtaining information which allows for the identification of the anonymous author. For the purpose of the present analysis, it will be sufficient to mention a few examples of such thresholds. Thus, in the United States, the most influential test is known as the Dendrite test, according to which “the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a *prima facie* basis” and “the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the *prima facie* case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed” (*Dendrite International v. Doe*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001)). Japanese law sets a more stringent standard, as stated in the text reproduced *infra*, note 13.

author may face embarrassment and may have to contend with a suit brought by the injured person.<sup>9</sup> The author also has interest in opposing disclosure in a forum which would not be remote or otherwise inconvenient.

The ISPs do not have inherent interest in maintaining the author's anonymity nor are they in a good position to defend his or her publication since they have no knowledge of the factual correctness of the infringing material and the author's belief in it. Their interest lies in avoiding liability towards the author for breaching their duty of confidentiality. The duty may be based on a contract with the author or any applicable statutes or case law. The ISPs may be exempted from liability and penalty for breaching the duty if they obey a court order for disclosure.<sup>10</sup> But they face double jeopardy if the disclosure order is not recognised in a state where their liability is pursued.

### III. Japanese Approach

Under Japanese law, the legal basis for a disclosure order is a statutory right against ISPs. The statute<sup>11</sup> essentially says that disclosure may be demanded of ISPs<sup>12</sup> if (1) the alleged infringement has clearly taken place and (2) there is a justifiable reason for obtaining the disclosure, as in the cases where the information sought is necessary to claim damages from the anonymous author.<sup>13</sup> Being a substantive (non-procedural) right, it may be asserted in and outside courts.

---

<sup>9</sup> While those consequences are the same in the cases of infringement of copyright, M. FULLER in his article, *Jurisdictional Issues in Anonymous Speech Cases* (2015) 31 *Communications Lawyer* 24, observes that the right to anonymity is negligible in such cases unlike the cases involving the right to free speech.

<sup>10</sup> As made explicit by, for example, s. 8 of the Irish Data Protection Act 1988, which provides:

“Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is –

[...]

(e) required by or under any enactment or by a rule of law or order of a court, [...]”

<sup>11</sup> The Act on the Limitation of Liability of the Providers of Specified Telecommunication Services and the Right to Demand the Disclosure of Information Enabling the Identification of the Sender.

<sup>12</sup> The ISPs against whom disclosure is sought must seek the opinion of the author unless the latter cannot be contacted or there are special circumstances (Art. 4(2) of the Act, *ibid.*).

<sup>13</sup> Art. 4(1) of the Act, *ibid.*, which reads in pertinent part (the present author's translation):

“Any person alleging that his or her rights were infringed by the circulation of information via specified telecommunications may, only in the cases falling within both the following items, demand the service provider of the specified telecommunications [...] (hereinafter referred to as the “provider of disclosure-related services”) to disclose information enabling the identification of the sender pertaining to the infringement of the rights (namely, information, including the name and address, contributing to the

## A. Choice of Law Question

Being a substantive right, this right may be asserted only where Japanese law is applicable. Under the Japanese choice-of-law rules, it is generally assumed by commentaries that the claim based on this right is characterised as tort,<sup>14</sup> with the result that Japanese law is normally applicable in the cases where the person injured from defamation is habitually resident in Japan.<sup>15</sup> But the tort characterisation is somewhat awkward since the claim is not meant to pursue tort liability of ISPs themselves. It is only a preliminary step to claiming the author's tortious liability. It seems preferable to see this statutory right as emanating from an overriding mandatory rule of the forum which is applicable irrespective of any choice-of-law rules.<sup>16</sup>

It is possible that where an ISP is subject to the obligation of disclosure under Japanese law, its relationship with the anonymous author is governed by a different legal system. To avoid double jeopardy, it must be possible to interpret the latter as allowing the ISP's duty of confidentiality towards the author to be discharged by reason of its obligation of disclosure towards the injured person. To avoid double jeopardy in other states, the recognition of the Japanese order of disclosure would have to be sought there.

---

identification of the sender of the offending information as stipulated by the applicable ordinance of the Ministry of Internal Affairs and Communications [...] which is possessed by the provider of disclosure-related services if:

- (i) there is clear evidence that the rights of a person demanding disclosure have been infringed by the circulation of the offending information; and
- (ii) the information enabling the identification of the sender is necessary for the person demanding disclosure to exercise his or her rights to claim damages or where there is any other justifiable reason for that person to obtain disclosure.<sup>17</sup>

<sup>14</sup> E.g. TELECOMMUNICATIONS CONSUMER POLICY DIVISION OF THE TELECOMMUNICATIONS BUREAU IN THE MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, *Act on the Limitation of Liability of the Providers*, enlarged and revised edition 2014, p. 102 (in Japanese) and K. IIDA, *Commentary on the Act on the Limitation of Liability of the Providers*, 2002, p. 116 (in Japanese).

<sup>15</sup> This results from Art. 19 of the Japanese choice-of-law legislation, *Hō no Tekiyō ni Kansuru Tsūsoku Hō* (Act Concerning the General Rules for the Application of Laws), which provides that liability for defamation is governed by the law of the injured person's habitual place of residence (or, if the injured person is an association or a foundation which is incorporated or unincorporated, the law of its principal place of business). An exception is stipulated in Art. 20. For details, see K. TAKAHASHI, *A Major Reform of Japanese Private International Law* (2006) 2 J Priv Int L 311, 331.

<sup>16</sup> In Japan, there is no statutory definition of the concept of overriding mandatory rules. The present author favours a broad definition of the concept, understanding it to mean the rules which by legislative intent are applicable to any situation falling within their scope irrespective of the law otherwise applicable pursuant to the choice-of-law rules.

## B. Jurisdictional Question

Where this statutory right is asserted in court, the question of jurisdiction arises. Since the ISPs keep an access log (IP addresses and time stamps) for only a limited duration, the usual practice in Japan is to seek a disclosure order corresponding to ② in FIGURE above under an expedited procedure for interim relief of protection.<sup>17</sup> To obtain such orders against foreign ISPs<sup>18</sup> such as Twitter and Facebook, a ground of jurisdiction known as the “doing business” jurisdiction has proven to be useful.<sup>19</sup> It is contained in Art. 3-3 of the Code of Civil Procedure (*Minji Soshō Hō*), which provides in the relevant part (the present author’s translation):

“The suits set out in each item below may be filed with the courts of Japan in the circumstances described in each of them.

[...]

(v) a suit against a person doing business in Japan (including a foreign company (as defined by Article 2(2) of the Companies Act (Act No. 86 of 2005)) which continuously carries out transactions in Japan): in the circumstances where the suit relates to the business in Japan.”

This head of jurisdiction is available for proceedings on the merits but it is also capable of providing jurisdiction for interim proceedings since, according to the Civil Interim Relief Act (*Minji Hozen Hō*),<sup>20</sup> the Japanese courts have jurisdiction to grant interim relief where they would have jurisdiction should the same relief be sought in proceedings on the merits. Since this head of jurisdiction does not prescribe the method of “doing business,” it is a broad ground of jurisdiction capable of capturing defendants who have no fixed place of business in Japan but conduct business in Japan by online means from outside Japan. Foreign ISPs come within

---

<sup>17</sup> An order corresponding to ③ in FIGURE above may only be sought in proceedings on the merit since the subscriber’s name is more sensitive information than the IP address.

<sup>18</sup> A writ of summons for interim proceedings need not be served but may be notified in appropriate means (Art. 3 of the Civil Interim Relief Rules (*Minji Hozen Kisoku*)). In practice, they are often sent through an international postal channel, a method which cannot be used for the cross-border service of documents under the Japanese Code of Civil Procedure (M. NOMURA, *Actual Practice of Handling Interim Proceedings in Internet-Related Cases at the Civil 9<sup>th</sup> Division of the Tokyo District Court* (2014) 1395 *Hanrei Times* 25, 34 (in Japanese)).

<sup>19</sup> According to various news sources, disclosure orders were issued by the Tokyo District Court against FC2 (Nevada company) on 6 February 2013, Twitter (California company) on 4 July 2013 and on 30 September 2015 and Facebook (Irish company) on 19 August 2014. None of those orders has been published in law reports but the text of the order against Twitter dated 4 July 2013 is to be found at <<https://www.chillingeffects.org/notices/1456984>> (accessed on 19 February 2016).

<sup>20</sup> Article 11 of the Act provides (the present author’s translation):

“A petition for an order of interim relief may be made only where a suit on the merits can be filed with the courts of Japan or where the property to be provisionally seized or the object of the dispute is present in Japan.”

this jurisdiction if they conduct business in Japan by providing their internet services to Japanese residents, the use of Japanese language being a good *indicium*.<sup>21</sup> Without this head of jurisdiction, it would be difficult to find jurisdictional grounds to obtain disclosure orders against foreign ISPs. Thus, the home-court jurisdiction,<sup>22</sup> for example, is not available if the ISP is a foreign company.<sup>23</sup> Among the claim-based jurisdictional rules, the rule for contractual claims<sup>24</sup> is inapplicable since there is no contract between the injured person and the ISP. The jurisdictional rule for tort claims<sup>25</sup> is not available since the claim for disclosure is founded on a special statutory right.<sup>26</sup> The “doing business” jurisdiction, on the other hand, is available irrespective of the legal nature of the claim, provided that the suit relates to the business in Japan.<sup>27</sup> Typical suits envisaged by this head of jurisdiction are

---

<sup>21</sup> The availability of this head of jurisdiction in such circumstances in the practice of Tokyo District Court is confirmed by Judge M. NOMURA, writing extra-judicially in his article mentioned in *supra* (note 18), at 27.

<sup>22</sup> The Japanese courts have general jurisdiction, *i.e.* jurisdiction available irrespective of the cause of action, where the defendant’s principal place of business is situated in Japan (Art. 3-2(3) of the Code of Civil Procedure).

<sup>23</sup> Where the foreign ISP has a Japanese subsidiary, the latter is subject to the home-court jurisdiction. But a disclosure order cannot be obtained if, as is often the case with foreign ISPs providing hosting services, the Japanese subsidiary is only engaged in marketing and has no control over the information sought.

<sup>24</sup> It is contained in Art. 3-3 of the Code of Civil Procedure, which provides in the relevant part (the present author’s translation):

“The suits set out in each item below may be filed with the courts of Japan in the circumstances described in each of them.

(i) An action for the enforcement of a contractual obligation, [...] or any other action relating to a contractual obligation:

– when the place of performance of the obligation as specified in the contract is located in Japan or when the place of performance of the obligation is located in Japan according to the governing law chosen in the contract. [...].”

<sup>25</sup> It is also contained in Art. 3-3 of the Code of Civil Procedure, which provides in the relevant part (the present author’s translation):

“The suits set out in each item below may be filed with the courts of Japan in the circumstances described in each of them.

[...]

(viii) a suit relating to a tort: when the tort occurred in Japan (except where the result of a harmful act committed abroad has occurred in Japan and the occurrence of that result in Japan would not have been normally foreseeable).”

<sup>26</sup> For the same view, see M. FUKUSHIMA, Internet related cases viewed from the standpoint of a judge in charge of interim proceedings II (2013) 13(9) LIBRA (The Tokyo Bar Association journal) 9, 13 (in Japanese); TELECOMMUNICATIONS CONSUMER POLICY DIVISION OF THE TELECOMMUNICATIONS BUREAU IN THE MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, *supra* (note 14), at 102 (in Japanese). Interestingly, the latter shows no discomfort in adopting the tort characterisation for choice-of-law purposes; See *supra* (note 14).

<sup>27</sup> Compared to the traditional US version of “doing business” jurisdiction, the Japanese version is more restrictive as it requires the suit to relate to the defendant’s business in Japan. For a fuller comparison, see K. TAKAHASHI, The Jurisdiction of Japanese Courts in a Comparative Context (2015) 11 J Priv Int L 103, 113.

those based on contractual obligations arising from “doing business” in Japan. But it is not impossible to regard a suit seeking disclosure of information enabling the identification of an anonymous author as relating to the ISP’s business in Japan.

## IV. French Approach

In French law, disclosure orders may be based on a provision in the Trust in Digital Economy Act,<sup>28</sup> promulgated in 2004. Article 6 II reads as follows:<sup>29</sup>

“(1) The persons mentioned in the first and second paragraphs of I [which may be understood to signify ISPs – note by the present author] hold and retain the information enabling the identification of any person who has contributed to the creation of the content of services of which they are providers.

[...]

(3) The judicial authority may require the providers mentioned in the first and second paragraphs of I to disclose the information mentioned in the first paragraph.”

To obtain disclosure, another possibility is to rely on a general rule of civil procedure. Article 145 of the Code of Civil Procedure (*Code de procédure civile*) provides for preparatory inquiries (*mesures d’instruction in futurum*), and reads as follows:<sup>30</sup>

“If there is a legitimate reason to preserve or to establish, before any legal process, the evidence of facts upon which the resolution of a dispute may depend, legally permissible preparatory inquiries may be ordered at the request of any interested party, by way of an *ex parte* application or summary procedure.”

---

<sup>28</sup> “Loi n° 2004-575 pour la confiance dans l’économie numérique”.

<sup>29</sup> The present author’s translation. The original French text reads in the corresponding part:

“(1) Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l’identification de quiconque a contribué à la création du contenu ou de l’un des contenus des services dont elles sont prestataires”.

[...]

“(3) L’autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa”.

<sup>30</sup> The original French text reads:

“S’il existe un motif légitime de conserver ou d’établir avant tout procès la preuve de faits dont pourrait dépendre la solution d’un litige, les mesures d’instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé”.



The application of those rules became an issue in a recent case seeking disclosure from Twitter.

**A. *UEJF v. Twitter*<sup>31</sup>**

In *UEJF v. Twitter*, the French Union of Jewish Students (UEJF) complained of numerous anti-Semitic tweets and sought disclosure from Twitter. Twitter, a California company, did not contest the French jurisdiction. But it argued that it was not subject to the obligation to retain information under the French Trust in Digital Economy Act, stating that it was doing no more than required by the law of California. Twitter also contended that the provisions of this Act were not overriding mandatory rules (*loi de police*) within the meaning of Article 3 of the Civil Code (*Code civil*).<sup>32</sup>

The Paris High Court noted that under a relevant decree, the retention of the information enabling the identification of authors was subject to another Act, the 1978 Act on Computers, Files and Liberties,<sup>33</sup> which was in its terms subject to the principle of territoriality. In that regard, it was not demonstrated that Twitter used material or human means in the territory of France to retain the information sought. The Court also acknowledged that for a rule to qualify as the *loi de police*, its application must be uncontestedly mandatory for safeguarding the nation's socio-economic structure, remarking that the fact that the breach of the rule would attract criminal sanctions was not sufficient. Having regard to all the circumstances, the Court concluded that it was not demonstrated, with sufficient evidence required of a summary procedure, that Article 6 II of the Act was applicable in the present case. The Court instead relied on Article 145 of the Code of Civil Procedure to order disclosure, making a brief remark that the provision was applicable in international cases.

On appeal, the Paris Court of Appeal affirmed the decision of first instance without considering the questions of choice of law and jurisdiction.

**B. Comments**

It is regretful that the Court of Appeal did not take the opportunity to clarify the circumstances in which Article 6 II of the Trust in Digital Economy Act would be

---

<sup>31</sup> TGI Paris, 24 janv. 2013, n° 13/50262, (2013) D. 300 An appeal lodged by Twitter was rejected by CA Paris, 12 juin 2013, n° 13/06106, (2013) D. 1614.

<sup>32</sup> Art. 3(1) provides (translation taken from the site of <<http://www.legifrance.gouv.fr/>> (accessed on 4 January 2016)):

Statutes concerning public policy and safety are binding on all those living on the territory.

The original French text reads:

“Les lois de police et de sûreté obligent tous ceux qui habitent le territoire”.

<sup>33</sup> “Loi n° 78-12 relative à l’informatique, aux fichiers et aux libertés”.

applicable to foreign ISPs.<sup>34</sup> A few commentators have doubted the correctness of the High Court's reliance on the territoriality principle provided by the 1978 Act, questioning whether it has any bearing on the disclosure, as distinguished from retention, of information sought under the Trust in Digital Economy Act.<sup>35</sup> Another commentator, apparently on the understanding that the Trust in Digital Economy Act imposes the obligation to disclose information as retained under the same Act, contrasts it with Article 145 of the Code of Civil Procedure which, according to her interpretation, requires disclosure of so much of the information as retained under the applicable, possibly foreign, law.<sup>36</sup>

Being a procedural rule, Article 145 of the Code of Civil Procedure should raise no choice-of-law question. It should be applicable as forming part of the *lex fori* where the French courts have jurisdiction as to the substance of the matter.<sup>37</sup> Where jurisdiction as to the substance exists under the Brussels I-bis Regulation,<sup>38</sup> this view finds a few supporting remarks in the case law of the CJEU (Court of Justice of European Union).<sup>39</sup> Where the court is not yet seized of the substance, the question to be asked is whether it would have jurisdiction when it is seized.<sup>40</sup> By hypothesising a suit against the author, it would be possible to see whether the French courts have jurisdiction on the basis that the offending online content could be viewed in France.<sup>41</sup>

---

<sup>34</sup> For the same view, see F. CHAFIOL-CHAUMONT/ A. CANIVEZ, *Affaire Twitter c/ UEJF: suite et fin?* (2013) 97 *Revue Lamy Droit de l'Immatériel* 31.

<sup>35</sup> C. MANARA, *Twitter: communication de données d'identification* [2013] *Recueil Dalloz* 300; A. COUSIN, *Twitter peut-elle échapper à la loi française?* [2013] *Recueil Dalloz* 696.

<sup>36</sup> F. CHAFIOL-CHAUMONT, *Messages racistes sur internet: Twitter devra communiquer les données permettant d'identifier les auteurs des tweets antisémites* (2013) 91 *Revue Lamy Droit de l'Immatériel* 26.

<sup>37</sup> For the same view, see H. GAUDEMET-TALLON, *Compétence et exécution des jugements en Europe: règlement 44/2001, conventions de Bruxelles (1968) et de Lugano (1988 et 2007)*, 4<sup>th</sup> ed. 2010, p. 322.

<sup>38</sup> Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.

<sup>39</sup> Case C-391/95, *Van Uden v. Deco-Line*, [1998] ECR I-7091, para. 22; Case C-99/96, *Mietz*, [1999] ECR I-2277, para. 41.

<sup>40</sup> A. NUYTS, *Le règlement communautaire sur l'obtention des preuves, un instrument exclusif?* [2007] *Rev. crit. dr. int.* pr. 53, 65; E. PATAUT [2005] *Rev. crit. dr. int.* pr. 742, 748 (Note on *St Paul Daily*).

<sup>41</sup> Case C-161/10, *eDate Advertising and Others*, [2011] ECR I-10269, according to which the courts of each Member State in the territory of which the online content infringing personality rights is or has been accessible have jurisdiction in respect of the damage caused in the territory of that Member State. The same conclusion seems to result from the French national rules of jurisdiction. Thus, commenting on the *UEJF v. Twitter* case, Th. FOURREY, *Twitter et le droit de la presse* (2014) 109 *Revue Lamy Droit de l'Immatériel* 67, 68, has argued that the application of Art. 145 would have been better justified on the basis that the French courts had jurisdiction under Art. 46 of the same Code, reasoning that damage had been suffered in France in the sense that the offending tweets had been received there.

Even if the courts of another EU Member State have, and the French courts do not have, jurisdiction as to the substance of the matter, “such provisional, including protective, measures” as may be available under French law may be sought in France pursuant to Article 35 of the Brussels I-bis Regulation. Do the preparatory inquiries under Article 145 of the French Code of Civil Procedure constitute “provisional, including protective, measures” within the meaning of that provision? According to the CJEU in *Reichert and Kockler*, that notion refers to “measures which [...] are intended to preserve a factual or legal situation so as to safeguard rights the recognition of which is sought elsewhere from the court having jurisdiction as to the substance of the matter.”<sup>42</sup> But according to another CJEU decision, *St. Paul Dairy Industries v. Unibel Exser*, it does not cover “a measure ordering the hearing of a witness for the purpose of enabling the applicant to decide whether to bring a case, determine whether it would be well founded and assess the relevance of evidence which might be adduced in that regard.”<sup>43</sup> When the latter decision was given, the question referred to the CJEU mentioned, in particular, orders enabling the advance clarification with regard to the identification of the party against whom proceedings must be instituted.<sup>44</sup> It might, therefore, be inferred from this ruling that orders for disclosure of information allowing for the identification of anonymous authors do not constitute “provisional, including protective, measures.”<sup>45</sup> This interpretation might seem supported by Recital 25 of the Regulation which states, “[t]he notion of provisional, including protective, measures should include, for example, protective orders aimed at obtaining information or preserving evidence as referred to in Articles 6 and 7 of Directive 2004/48/EC [...] on the enforcement of intellectual property rights.” It does not mention Article 8 of the same Directive which refers to orders aimed at obtaining such information as the name of the producer of goods infringing an intellectual

---

Art. 46 provides in the relevant part (translation taken from the site of <<http://www.legifrance.gouv.fr/>> (accessed on 4 January 2016)):

“The plaintiff may bring his case, at his choosing, besides the court of the place where the defendant lives, before:

[...]

- in tort matters, the court of the place of the event causing liability or the one in whose district the damage was suffered; [...].”

The original French text reads in the corresponding part:

“Le demandeur peut saisir à son choix, outre la juridiction du lieu où demeure le défendeur:

[...]

- en matière délictuelle, la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi; [...].”

<sup>42</sup> Case C-261/90, [1992] ECR I-2149, para. 34.

<sup>43</sup> Case C-104/03, [2005] ECR I-3481.

<sup>44</sup> A Dutch disclosure order. No further detail of the order is given in the judgment or the Advocate General’s Opinion.

<sup>45</sup> The Supreme Court of Ireland, too, held that a measure designed to disclose the identity of persons who might be sued could not be regarded as the type of measure which fell within this expression: *Ryanair Ltd v. Unister GmbH and by order Aeruni GmbH* [2013] IESC 14, para. 10.3.

property right, a type of order similar in purpose to those for the disclosure of information enabling the identification of infringers of personality rights. It seems, however, that Recital 25 in its entirety should be read as confirming the distinction introduced by the decision in *St. Paul Dairy* between measures aimed at preserving evidence and measures intended merely to obtain evidence.<sup>46</sup> In this regard, where the identity of anonymous online authors is sought to be uncovered, the disclosure of the time stamps of the anonymous posts and the IP addresses used may be sought in interim proceedings to preserve the log of those details which might otherwise be deleted by the internet access provider after a period of time. In such cases, the orders should be considered to constitute “provisional, including protective, measures” since they are “measures which [...] are intended to preserve a factual or legal situation.”<sup>47</sup> If this interpretation is accepted, it should be noted that the granting of provisional or protective measures under Article 35 of the Brussels I-*bis* Regulation is conditional on “the existence of a real connecting link between the subject matter of the measures sought and the territorial jurisdiction of the [Member] State of the court before which those measures are sought.”<sup>48</sup> Though exactly what is required by this condition is unclear when the measure does not concern the seizing of property,<sup>49</sup> it would hardly be met if the ISP stores the information sought to be disclosed outside the jurisdiction.

Even where the French courts have jurisdiction over a potential suit against the author, a separate question arises: whether the French courts have power to make an extraterritorial order,<sup>50</sup> requiring ISPs to disclose information located abroad. Such an order might seem contrary to the spirit of the French blocking statute.<sup>51</sup> It provides as follows in Article 1*bis*:<sup>52</sup>

---

<sup>46</sup> For the same view, see F. WILKE, *The impact of the Brussels I Recast on important “Brussels” case law* (2015) 11 J Priv Int L 128, 139.

<sup>47</sup> *Reichert and Kockler* (note 42). E. PATAUT (note 40), at 750 and 751, considers that preparatory inquiries under Art. 145 are largely excluded from “provisional, including protective, measures” but acknowledges that there can be exceptions justified by the imminent risk of destruction of evidence, noting that Art. 145 has dual objectives, namely to avoid the deterioration of evidence and to assess the chances of success at trial, the first of which attracts the application of what is now Art. 35 of the Brussels I-*bis* Regulation.

<sup>48</sup> Case C-391/95, *Van Uden* [1998] ECR I-7091.

<sup>49</sup> For the same view, see the Commission Report on the application of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM(2009) 174 final) para. 3.6.

<sup>50</sup> This corresponds to the question addressed *infra* (heading VI.B. “jurisdiction to prescribe”) in the context of English law.

<sup>51</sup> “Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères” (Act relating to the communication of documents or information in economic, commercial, industrial, financial or technical matters to foreign natural or legal persons).

<sup>52</sup> The present author’s translation. The original French text reads:

“Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou

“Subject to any treaties or international agreements and Acts and regulations in force, it is prohibited for any person to request, to investigate or to communicate in writing, orally or by any other means, documents or information in economic, commercial, industrial, financial or technical matters leading to the establishment of proof for the sake of foreign judicial or administrative proceedings or in the context of such proceedings.”

It seeks to ensure with a threat of criminal penalty<sup>53</sup> that recourse be made to the French Code of Civil Procedure<sup>54</sup> or the Hague Evidence Convention<sup>55</sup> of which France is a Contracting State, in order to collect information from France for the sake of foreign proceedings.<sup>56</sup> This Act is, however, hardly invoked in practice and has been described as “ineffective et obsolète.”<sup>57</sup> It is, in fact, not unprecedented for the French courts to order Article 145 inquiries to be conducted outside France without resorting to the Hague Evidence Convention.<sup>58</sup>

---

renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.”

<sup>53</sup> Provided in Art. 3.

<sup>54</sup> Arts. 736 to 748 of the French Code of Civil Procedure.

<sup>55</sup> Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.

<sup>56</sup> The French government views recourse to the Hague Evidence Convention as mandatory where the evidence is located in another Contracting State: France's response to the Questionnaire of May 2008 drawn up by the Permanent Bureau of the Hague Conference on Private International Law relating to the Hague Evidence Convention (2008), p. 13.

<sup>57</sup> B. CARAYON, Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la proposition de loi (N° 3985) de M. Bernard Carayon visant à sanctionner la violation du secret des affaires, Assemblée Nationale No. 4159 (2012), p. 22.

<sup>58</sup> Apart from *UEJF v. Twitter*, examined above, see e.g. *Societe Luxguard v. Societe SN Sitracco and Another* [1996] I.L.Pr. 5, in which the Versailles Court of Appeal affirmed an order appointing an expert to go to a building and inspect its works in Spain (criticised by G. COUCHEZ [1995] Rev. crit. dr. int. pr. 80, 87). The Court considered that the Hague Evidence Convention, though regulating letters rogatory, was not applicable to a probative measure (*mesure d'ordre probatoire*), provided that it would not infringe the sovereignty of another Contracting State. On that basis, the Court found that the task of the appointed expert, being purely technical, would not amount to the administration of evidence which would involve the danger of infringing the sovereignty of Spain. It should be noted that this case preceded Regulation No 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters ([2001] OJ L174/1), which prevails over the Hague Evidence Convention in relations between the EU Member States (Art. 21(1)) and recourse to which has been held non-mandatory (Case C-332/11, *ProRail v. Xpedys and others* (2013)).

## V. US Approach

The approach in the United States, though not uniform in detail, is strikingly different from those in Japan and France. The anonymous author may be sued in the name of “John Doe”<sup>59</sup> and then a non-party discovery order, called “Doe subpoena,” may be issued to the ISPs to unmask “John Doe.” As it is a procedural order, it gives rise to no choice-of-law question. The US debate is focused on jurisdiction and, unlike the Japanese debate, jurisdiction over Doe rather than ISPs. The debate centres on whether it is premature to require any jurisdictional analysis before the identity of the defendant is revealed and, if not, where the injured person should bring his or her suit to make a sufficient showing of jurisdiction over Doe.

### A. Jurisdictional Analysis before Identification of Defendant

It appears that the only decision at the appellate level of federal courts which has squarely addressed this question is *AF Holdings v. Does* 1–1058.<sup>60</sup> In this case, the Court of Appeals for the DC Circuit acknowledged that to bring an action, a plaintiff has no obligation to establish personal jurisdiction until the defendant raises that defense. The Court, however, emphasized that different principles applied where a plaintiff did not just file a complaint but also sought a non-party discovery order to reveal the identity of the Doe defendants. It held that discovery would be denied unless the plaintiff has “a good faith belief that such discovery will enable it to show that the court has personal jurisdiction over the defendant.”<sup>61</sup> In the Court’s reasoning, absent such a threshold showing, there would be little reason to believe that the information sought would be “relevant to the subject matter involved in the action,” a general requirement for a discovery order<sup>62</sup> as provided by the Federal Rules of Civil Procedure 26(b)(1).<sup>63</sup> The Court explained that the identity of

---

<sup>59</sup> The practice of bringing a suit against “John Doe” is well established in federal courts as well as in a vast majority of state courts. The Federal Rules of Civil Procedure are largely silent or unclear on the practice but a majority of states have express provisions for it. For details, see C. RICE, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties* (1996) 57 U. Pitt. L. Rev. 883.

<sup>60</sup> 752 F.3d 990 (2014). This is a case on copyright infringement but the point discussed here would equally apply to cases involving the infringement of personality rights.

<sup>61</sup> For an earlier decision to the same effect, see *Nu Image v. Does* 1-23, 322, 799 F. Supp. 2d 34 (D.D.C. 2011) at 37 (a case on copyright infringement).

<sup>62</sup> The Court noted that where no party had yet been specifically named as a defendant, the only potential avenue for discovery was the Federal Rules of Civil Procedure 26(d)(1), which provided for discovery “by court order.”

<sup>63</sup> Rule 26(b)(1) has been amended with effect from 1 December 2015 and no longer contains the quoted wording. The amendment narrowed the scope of discovery by requiring it to be “proportional to the needs of the case.” In the context of the present discussion, the amendment will, if anything, only give a stronger support for the ruling that the plaintiff must “have at least a good faith belief that such discovery will enable it to show that the court has personal jurisdiction over the defendant.”

prospective defendants who would not be amenable to jurisdiction could be of little use. It should be noted that what the Court required the plaintiff to do was not to demonstrate that the trial court had personal jurisdiction over the anonymous defendant. Rather, it was merely to show a good faith belief that the trial court had jurisdiction.

The state courts follow the civil procedure rules of their own states. The Rules of Civil Procedure of Ohio, for example, permit pre-suit discovery that “is necessary to ascertain the identity of a potential adverse party” (Rule 34(D)(3)). Texas authorises the broadest form of pre-suit discovery, granting “a proper court” power to “investigate a potential claim” (Rule 202 of the Texas Rules of Civil Procedure). In a recent Texas case, *John Doe a/k/a “Trooper”*,<sup>64</sup> a petition was filed, requesting Google to disclose the identity of a pseudonymous blogger under Rule 202. The plaintiff sent notice to the blog email address.<sup>65</sup> The blogger filed an appearance without revealing his identity, asserting that his only contact with Texas was that the blog could be read on the Internet there. The Texas Supreme Court, in a 5-4 split decision, held that “a proper court” must have personal jurisdiction over the potential defendant. It acknowledged that the burden on the plaintiff could be heavy where the potential defendant’s identity was unknown. But the Court refused to “interpret Rule 202 to make Texas the world’s inspector general.” On that reasoning, the Court concluded that the trial court’s order authorising discovery exceeded its authority under Rule 202. But the Court did not articulate the jurisdictional standard applicable in this context. The dissenting opinion held that the question of personal jurisdiction was premature and impossible to answer when it was directed at an anonymous individual.<sup>66</sup> In its reasoning, a “court’s exercise of personal jurisdiction over a party is predicated on an analysis of his connections with the forum state” and “when a party chooses to remain anonymous, a court is powerless to evaluate his connection to the forum state.” This observation seems incontestable. It logically follows that the majority’s ruling that “a proper court” must have personal jurisdiction over the potential defendant could not be taken as insisting on a full-fledged jurisdictional analysis.

---

<sup>64</sup> 57 Tex. Sup. Ct. J. 1440 (2014).

<sup>65</sup> In the United States, the plaintiffs are generally required to make efforts to notify the anonymous author. Thus, in the *Dendrite International* case, the decision which established the most influential substantive test for disclosure in the United States (See *supra* (note 8)), it was held:

“[...] the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP’s pertinent message board.”

<sup>66</sup> The dissenting opinion cited some federal courts’ decisions which had made the same point. They are *AF Holdings, LLC v. Does* 1–162, 2012 WL 488217 (S.D.Fla. 2012); *Bloomberg, L.P. v. Does* 1–4, 2013 WL 4780036 (S.D.N.Y. 2013); *First Time Videos, LLC v. Does* 1–76, 276 F.R.D. 254 (N.D.Ill. 2011); and *Call of the Wild Movie, LLC v. Does* 1–1,062, 770 F.Supp.2d 332 (D.D.C. 2011).

## B. Where to Sue

Then, the next question which must be addressed is where the injured person should bring his or her suit to make a sufficient showing of jurisdiction over John Doe. In the cases of copyright infringement through file sharing, prior to filing suits against “John Doe” infringers, the record companies often know them by their IP addresses. This is because in order to facilitate file sharing, their IP addresses are distributed to fellow users, which the record companies can get hold of by monitoring the P2P network. Then, it is possible to approximately determine the infringer’s location through what is known as a geolocation service, a kind of service which makes it possible to estimate the location of internet users based on their IP addresses. Thus, in *AF Holdings v. Does* 1–1058, a DC circuit case examined above, the plaintiff conceded that “the only conceivable way that personal jurisdiction might properly be exercised over these Doe defendants is if they are residents of the District of Columbia or at least downloaded the copyrighted work in the District.”<sup>67</sup> The DC Circuit Court of Appeals held that the plaintiff abused the discovery process by not limiting its inquiry to those defendants who might actually be located in the District by using a geolocation service.<sup>68</sup> In the same way, in the cases involving the infringement of personality rights, if the injured person has got hold of the IP address used by the anonymous author and demands the internet access provider to reveal the name of the subscriber (③ in FIGURE above), it will not be difficult to estimate the area where the author has posted the online content and establish on a *prima facie* basis the jurisdiction of the courts there by relying on a rule giving jurisdiction to the courts where a tortious conduct has been committed (*loci actus*).

Then, could a sufficient showing of jurisdiction over an anonymous defendant be made where the IP address of the defendant is not known to the plaintiff, as is typically the case where the injured person seeks disclosure from the host of the server or website where infringing material has been posted (② in FIGURE above)?

Firstly, could such a showing be made by filing in the State where the tortious conduct was committed (*loci actus*)? In *Melvin v. Doe*,<sup>69</sup> the Virginia Circuit Court granted a motion to quash a subpoena against America On Line (AOL), a Virginia company. The Court found that the defendant, an anonymous author, fell within the *loci actus* rule of the Virginia Long Arm Statute by using AOL’s server in Virginia when publishing the defamatory content. But it held that the “minimum contacts” requirements of the Due Process Clause of the Fourteenth Amendment were not satisfied since the defamatory posting did not target Virginia but involved issues of local interest in Pennsylvania. This ruling may suggest that a sufficient showing cannot be made by suing an anonymous author in the State where the ISP’s server used to post the offending material is located. Such a conclusion,

---

<sup>67</sup> A reference was made to the DC long-arm statute providing for personal jurisdiction over a person “causing tortious injury in the District of Columbia.”

<sup>68</sup> This ruling was followed in other cases, e.g. *Malibu Media v. John Doe*, 2015 WL 5173890 (District Court for the District of Columbia).

<sup>69</sup> 1999 WL 551335 (Va. Cir. Ct.).



however, will not be inevitable since the court might not require a full-fledged jurisdictional analysis. Thus, in *Malcolm et al. v. Doe 1 et al.*,<sup>70</sup> a suit was filed in California to seek third party discovery against WordPress.com, a California company, which hosted an offending blog. The plaintiffs argued that the court had personal jurisdiction over Does because they had “purposefully avail[ed] themselves of the services of a company located in the State of California.” The California Court of Appeal affirmed the trial court’s decision to deny a motion to strike under the Californian anti-SLAPP statute. The Court, not discussing the plaintiff’s jurisdictional argument, apparently accepted it. This was notwithstanding that the plaintiffs were English local politicians and their aim was to learn if their political rival in England was the author of the blog.

Then, could a sufficient showing be made of jurisdiction over John Doe by filing in the State where the injury from tortious conduct was sustained (*loci damni*)? It has been suggested<sup>71</sup> that in defamation cases, knowledge of the defendant’s identity will not always be essential to a plaintiff’s *prima facie* showing of personal jurisdiction since the substance of the challenged publication may contain sufficient indicia of the defendant’s forum contacts. Thus, in *Melvin v. Doe*, examined above, after the Virginia Court granted a motion to quash the subpoena, the suit was re-filed in Pennsylvania, which the defendant’s publication targeted, and the court there took jurisdiction.<sup>72</sup>

## VI. English Approach

In England, the legal basis for a disclosure order for unmasking an anonymous online infringer of a personality right is the Norwich Pharmacal order.<sup>73</sup> In the leading case, unrelated to online infringement of personality rights, the House of Lords held:<sup>74</sup>

“If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers.”

---

<sup>70</sup> 2013 WL 1278957 (California Court of Appeal).

<sup>71</sup> M. FULLER (note 9).

<sup>72</sup> S. SPENCER, *Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace* (2001) 19 *John Marshall Journal of Computer & Information Law* 493, fn. 108.

<sup>73</sup> This is also true in Canada. See *e.g. York University v. Bell Canada Enterprises* [2009] O.J. No. 3689 (Ont. Super. Ct.).

<sup>74</sup> *Norwich Pharmacal Co. v. Customs and Excise Commissioners* [1974] AC 133, 203.

In England, unlike in the United States, pre-trial disclosure cannot be sought from non-parties to proceedings under what is known as the “mere witness” rule. The Norwich Pharmacal principle constitutes an exception to this general rule.<sup>75</sup> To obtain a Norwich Pharmacal order,<sup>76</sup> the person mixed up in the tortious acts of others can be named as a defendant solely for the purpose of obtaining discovery and without there being any cause of action against it.<sup>77</sup> Thus, to obtain information enabling the identification of an anonymous online author, the ISP may be named as a defendant.<sup>78</sup>

With respect to personal jurisdiction, unlike the cases of the United States where the debate is concentrated on jurisdiction over the anonymous author, the question of jurisdiction over ISPs was considered in a few English cases discussed below. In a few other cases, no question of jurisdiction was discussed as the ISPs did not resist the Norwich Pharmacal orders made against them.<sup>79</sup>

There appears to be no discussion of the choice-of-law question, presumably due to the procedural character of the Norwich Pharmacal order. What arises instead is the question of jurisdiction to prescribe, *i.e.* the territorial limit to the subject matter which English law as administered by an English judge can regulate.<sup>80</sup>

---

<sup>75</sup> The Norwich Pharmacal decision was greeted with astonishment in the legal profession as it had been felt to be “un-British” to allow litigants to trouble non-parties (L. HOFFMANN, *Changing Perspectives on Civil Litigation* (1993) 56 *Modern Law Review* 297, 300).

<sup>76</sup> The power to grant this order is based on the court’s inherent jurisdiction (J. O’HARE/K. BROWNE, *Civil Litigation*, 14<sup>th</sup> ed. 2009, para. 30.026), which is preserved by the Civil Procedure Rules (CPR) 31.18.

<sup>77</sup> *Mackinnon v. Donaldson Lufkin & Jenrette Securities* [1986] Ch. 482, 498 per HOFFMANN J.

<sup>78</sup> There appears, however, to be an unreported decision involving Facebook as the Norwich Pharmacal defendant, in which it was indicated that issuing a claim form against the defendant was unnecessary (A. CADDICK, *An effective global remedy* 160 (2010) *New Law Journal* 211).

<sup>79</sup> *E.g. Applause Store Productions & Firshat v. Raphael* [2008] EWHC 1781, para. 10 stating that a Norwich Pharmacal order was obtained against Facebook without discussing any jurisdictional question; *G v. Wikimedia Foundation* [2009] EWHC 3148, para. 38, the lawyers for the respondent stating, “[w]ithout waiving our insistence that no court in the United Kingdom has proper jurisdiction over us as a foreign entity, we nevertheless are willing to comply with a properly issued court order [...]”; *Daniel Hegglin v. Person(S) Unknown, Google Inc* [2014] EWHC 2808, para. 22, with Bean J stating, “Google were and remain willing to comply with any indication from me that a Norwich Pharmacal order would be justified without prejudice to their general arguments about service out of the jurisdiction. They raised no separate dispute under this heading.”

<sup>80</sup> Referred to by HOFFMANN J. in *Mackinnon v. Donaldson Lufkin & Jenrette Securities* [1986] Ch. 482, 493 as “subject matter jurisdiction.”

## **A. Personal Jurisdiction**

### **1. Lockton Companies International v. Persons Unknown, Google<sup>81</sup>**

In *Lockton Companies International v. Persons Unknown, Google*, a Norwich Pharmacal order was sought against Google, a company incorporated in Delaware and located in California. The court upheld jurisdiction over Google as “a necessary and proper party”<sup>82</sup> to the claim against the anonymous authors who constituted the first defendants.<sup>83</sup> Since the content of the offending e-mails related to an English company and to its employees, the court saw no difficulty in assuming jurisdiction over the first defendants, finding it reasonable to infer that that once they were identified, service would be effected on them within the jurisdiction. The court accepted the claimant’s submission that it would be necessary to obtain an order against Google to acquire information which would lead to the identification of the anonymous author.

### **2. Bacon v. Automattic and Others<sup>84</sup>**

In *Bacon v. Automattic and Others*, a Norwich Pharmacal order was sought against the defendants, US companies, who hosted the websites publishing defamatory statements. The anonymous author was not sued as a defendant. The claimant applied for permission to serve the claim forms out of the jurisdiction on the ground that a “claim [was] made for an injunction ordering the defendant to do [...] an act within the jurisdiction,”<sup>85</sup> namely, in the instant case, disclose the information sought in England. The court granted permission but did not discuss

---

<sup>81</sup> [2009] EWHC 3423.

<sup>82</sup> Para. 3.1(3) of Practice Direction 6B, supplementing CPR Pt 6 provides in the relevant part:

“The claimant may serve a claim form out of the jurisdiction with the permission of the court under rule 6.36 where –  
[...]

(3) A claim is made against a person (‘the defendant’) on whom the claim form has been or will be served (otherwise than in reliance on this paragraph) and –

(a) there is between the claimant and the defendant a real issue which it is reasonable for the court to try; and

(b) the claimant wishes to serve the claim form on another person who is a necessary or proper party to that claim.”

<sup>83</sup> It became possible to sue an unknown person in England by the 17<sup>th</sup> century: see C. RICE (note 59), at fn. 20.

<sup>84</sup> [2012] 1 W.L.R. 753.

<sup>85</sup> Para. 3.1(2) of Practice Direction 6B, supplementing CPR Pt 6 provides in the relevant part:

“The claimant may serve a claim form out of the jurisdiction with the permission of the court under rule 6.36 where –  
[...]

(2) A claim is made for an injunction ordering the defendant to do or refrain from doing an act within the jurisdiction.”

the question of jurisdiction since the central issue of the case was the permissibility of service of the claim form by e-mail.<sup>86</sup>

### 3. Comments

It has been suggested that the English courts may issue a Norwich Pharmacal order only if they have personal jurisdiction over the person against whom the order is made.<sup>87</sup> This is also the assumption taken by the decisions examined above.

Where the defendant is not domiciled in any EU Member State, jurisdiction may be obtained under the common law by service of a claim form. This is possible where the defendant is present in England, though the exercise of jurisdiction is subject to the principle of *forum non conveniens*. Whether the claim form could be served out of the jurisdiction has been doubted.<sup>88</sup> In particular, it has been questioned whether the head of jurisdiction for “an injunction ordering the defendant to do [...] an act within the jurisdiction” should be available to Norwich Pharmacal orders as it would give the English courts unlimited personal jurisdiction to make such orders.<sup>89</sup> In the cases involving online infringement of personality rights, however, it would seem possible to effect service on the ISP by regarding it as a necessary party to a claim against the anonymous author. The interest of the author, who has a greater stake in the case than the ISP,<sup>90</sup> is protected by being made the first defendant and by the requirement that “there is between the claimant and the defendant a real issue which it is reasonable for the court to try”<sup>91</sup> as well as the requirement that a claim form will be served on the defendant. Although it is not possible to conclusively determine whether the last requirement is fulfilled while the defendant remains anonymous, a reasonable inference, as made in the Lockton Companies International case, should be considered sufficient.

Where the defendant against whom a Norwich Pharmacal order is sought is domiciled in England, the English courts have jurisdiction under Article 4(1) of the Brussels I-bis Regulation. If the defendant is domiciled in another EU Member State or Contracting State of the Lugano Convention, it would seem difficult to find applicable jurisdictional rules in the Brussels I-bis Regulation or Lugano Convention<sup>92</sup> since there is no cause of action against the Norwich Pharmacal defendant. Like the English common law rules, the Regulation does contain a jurisdictional rule for multiple defendants.<sup>93</sup> It seems, however, less likely to be

---

<sup>86</sup> This issue arose because of the need for expeditious handling of the case. See *supra* (note 18) for the way things are done in Japan.

<sup>87</sup> T. HARTLEY, *Jurisdiction in conflict of laws – disclosure, third-party debt and freezing orders* (2010) 126 LQR 194, 203.

<sup>88</sup> *Ibid.*

<sup>89</sup> *Ibid.* This view was expressed prior to the Bacon decision, examined above.

<sup>90</sup> As discussed under *supra* (heading II).

<sup>91</sup> Para. 3.1(3)(a) of Practice Direction 6B (note 82).

<sup>92</sup> For the same view, see T. HARTLEY (note 87).

<sup>93</sup> Art. 8(1). Article 8 provides in the relevant part:

available since it requires that “the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings,” a requirement which is unlikely to be satisfied by a claim seeking a Norwich Pharmacal order.

## **B. Jurisdiction to Prescribe**

It is well established that parties to proceedings in England are not excluded from the obligation to disclose documents in their “control” (as defined by CPR 31.8(2)) just because those documents are in a foreign state.<sup>94</sup> On the other hand, the power to obtain disclosure from non-party banks under section 7 of the Bankers' Books Evidence Act 1879<sup>95</sup> cannot, save in exceptional circumstances, be exercised to require the production of documents situated in a foreign state as it would involve the infringement of the sovereignty of the foreign state.<sup>96</sup> It has been argued that the latter principle should apply when making a Norwich Pharmacal order on the reasoning that although in form such an order requires disclosure by a party, in substance it is an order against a non-party.<sup>97</sup> It should be noted, however, that in the decisions examined above, no territorial limitation was placed on the Norwich Pharmacal orders.

---

“A person domiciled in a Member State may also be sued:

(1) where he is one of a number of defendants, in the courts for the place where any one of them is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings; [...].”

<sup>94</sup> *Mackinnon v. Donaldson Lufkin & Jenrette Securities* [1986] Ch 482, 494 with HOFFMANN J. stating, “[i]f you join the game, you must play according to the local rules.”

<sup>95</sup> It provides:

“On the application of any party to a legal proceeding a court or judge may order that such party be at liberty to inspect and take copies of any entries in a banker's book for any of the purposes of such proceedings. An order under this section may be made either with or without summoning the bank or any other party, and shall be served on the bank three clear days before the same is to be obeyed, unless the court or judge otherwise directs.”

Unlike Norwich Pharmacal orders, orders under this provision are available only where proceedings have been commenced: see W. KENNETT, *The enforcement of judgments in Europe* (2000) p. 117.

<sup>96</sup> *Mackinnon v. Donaldson Lufkin & Jenrette Securities* [1986] Ch 482.

<sup>97</sup> LORD COLLINS *et al.* (ed.), *Dicey, Morris & Collins on the Conflict of Laws*, 15<sup>th</sup> ed. 2012, para. 8-073; HOFFMANN J. in the *Mackinnon* case, *ibid.*, seemed to have the same view, observing at 498 “for the purposes of the jurisdictional rules now under consideration, the *Norwich Pharmacal* case is much more akin to the subpoena directed to a witness than the discovery required of an ordinary defendant.”

## VII. Cross-Border Enforcement of Disclosure Orders

With the questions of choice of law and jurisdiction having been examined, the following analysis will address the enforcement of disclosure orders.

### A. Necessities for Cross-Border Enforcement

It may be necessary to enforce disclosure orders abroad for two reasons. Firstly, ISPs may refuse to comply with a disclosure order unless it is issued by the courts of their home country.<sup>98</sup> Thus, in the English case of *Bacon v. Automattic*, examined above,<sup>99</sup> one of the defendants was Wikimedia, a California foundation. It stated:<sup>100</sup>

“Unfortunately, the Wikimedia foundation does not disclose personally identifying information regarding its users absent US subpoena. Please note that we do not comply with foreign subpoenas<sup>101</sup> absent and [*sic*] immediate threat to life or limb, due to the varying standards and requirements of courts from country to country. There is a

---

<sup>98</sup> This is not always the case. In *UEJF v. Twitter*, examined *supra* (note 31), after the disclosure order was affirmed by CA Paris, Twitter disclosed the information sought (F. CHAFIOL-CHAUMONT/ A. CANIVEZ (note 34)). This is notwithstanding that Twitter, being a California company and maintaining its servers in the United States, was subject to the law of the United States and consequently benefited from the guarantee of the freedom of expression under the First Amendment of the US Constitution, which is perceived to be more extensive than under French law (J. FRANCILLON, Messages racistes ou antisémites postés sur le réseau social Twitter (2013) *Revue de sciences criminelles et de droit pénal comparé* 566). An example of elaborate terms indicating the possibility of complying with a foreign court order can be found in the Privacy policy statement of Instagram, a California company (<<https://instagram.com/about/legal/privacy/>>, last accessed on 22 February 2016), which states:

“We may [...] share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.”

<sup>99</sup> *Supra* (note 84).

<sup>100</sup> At para. 13.

<sup>101</sup> Another episode of non-compliance is presented in RAJAH & TANN LLP, Pre-action Interrogatories and Discovery (April 2013 <<http://eoasis.rajahtann.com/eoasis/lu/pdf/2013-04-Interrogatories-s%284%29.pdf>>, last accessed on 22 February 2016). According to this source, a footballer involved in newspaper reports obtained an injunction to protect him from being identified. After his name was revealed on Twitter in breach of the injunction, the footballer sought a Norwich Pharmacal order against Twitter to reveal the identities of those who had breached the injunction. Twitter, being based in the United States, refused to comply and the footballer abandoned to pursue his claim against the Twitter users.

procedure by which you can have a foreign subpoena recognized by US courts. Should you choose to pursue this course of action, please send the US subpoena to me and we will comply with the subpoena to the best of our ability.”<sup>102</sup>

Another reason for the need to enforce a disclosure order abroad is the limitation which exists on enforcement jurisdiction in the State in which the order is made. While courts may make extra-territorial disclosure orders,<sup>103</sup> the enforcement of such orders is another matter.<sup>104</sup> The limitation on enforcement jurisdiction protects the non-party witness since non-compliance with disclosure orders could otherwise result in sanctions.<sup>105</sup> Thus, in a recent case,<sup>106</sup> the Virginia Circuit Court held Yelp, a California company, in civil contempt for refusal to comply with a Doe subpoena which had been issued earlier in Virginia. On appeal, the Virginia Supreme Court vacated the contempt order, holding that the Virginia courts lacked authority to compel non-resident<sup>107</sup> non-parties to produce documents located outside of Virginia.<sup>108</sup> But the Court did not quash the subpoena, reasoning that the plaintiff might choose to seek enforcement of the subpoena in California.

## **B. Enforcement of Foreign Disclosure Orders in California**

The conditions and procedure for the enforcement of foreign disclosure orders depend on the law of the requested state. The present article focuses on the law of

---

<sup>102</sup> As will be examined below, it is possible to have a subpoena issued in California on the basis of a foreign discovery order. But it is also possible to file a motion to quash the resulting California subpoena. The quoted statement of Wikimedia does not seem to rule out the possibility of filing such a motion.

<sup>103</sup> As discussed at the text accompanying *supra* (note 50) in the context of French law and at *supra* (heading VI.B.) in the context of English law.

<sup>104</sup> F. MANN, *The Doctrine of Jurisdiction in International Law* (1964) 111 *Recueil des Cours* 1, 137, states:

“There is, it is true, no objection to a State, by lawful means, [...] requiring a foreign witness to appear for the purpose of giving evidence. But the foreign witness is under no duty to comply, and to impose penalties upon him and to enforce them against his property or against him personally on the occasion of a future visit constitutes an excess of criminal jurisdiction and runs contrary to the practice of States in regard to the taking of evidence as it has developed over a long period of time.”

<sup>105</sup> M. FULLER (note 9).

<sup>106</sup> *Yelp v. Hadeed Carpet Cleaning*, 770 S.E.2d 440 (2015).

<sup>107</sup> Yelp did not have an office in Virginia. The Court left open the position with respect to a non-party foreign corporation maintaining an office in Virginia.

<sup>108</sup> This ruling is consistent with the Brief of Amici Curiae filed in support of Yelp by Automattic, Facebook, Google, Tripadvisor and Twitter (2015). They argued in one voice that “[t]he territorial limitation on states’ subpoena power has always been and remains well-grounded in law and sound as a matter of public policy.”

California as it is home to many major ISPs, as demonstrated by the facts of many cases discussed above.

Where a subpoena has been issued in a state of the United States, it is enforceable in California under the Interstate and International Depositions and Discovery Act,<sup>109</sup> which entered into force in 2010. The Act eliminates the need for obtaining letters rogatory (letters of request) and establishes a simple clerical procedure, under which a California subpoena is issued, incorporating the terms of a subpoena issued in another state by way of the submission of the latter to a court clerk in California.<sup>110</sup> As it is not necessary to obtain local counsel,<sup>111</sup> the procedure is cost-effective. The newly issued subpoena is enforceable in California but it is also challengeable there by a motion to quash under the law of California.<sup>112</sup> The Act is modelled on the Uniform Interstate Depositions and Discovery Act<sup>113</sup> which was created in 2007 and has been enacted in a majority of the states of the United States. The Californian Act, however, departs from the Uniform Act on the scope of application. The prefatory note of the Uniform Act states:<sup>114</sup>

“The [drafting] committee decided not to extend this Act to include foreign countries [...] The committee felt that international litigation is sufficiently different and is governed by different principles, so that discovery issues in that arena should be governed by a separate act.”

The Californian Act, on the other hand, clarifies through the definition of the words “foreign jurisdiction”<sup>115</sup> that it is applicable not just to subpoenas of other states of the United States but also to those of other nations. Accordingly, in the English case of *Bacon v. Automattic*, examined above,<sup>116</sup> a California counsel gave a statement stating, “a Norwich Pharmacal order may be enforced in California as provided in the recently enacted [...] Act.” If, however, a motion to quash the resulting California subpoena is filed, it is not clear how it is to be decided under the law of California. No authority seems as yet to have developed on the point. It is not unimaginable for such a motion to be granted in favour of the right to

---

<sup>109</sup> §§ 2029.100 *et seq.* of the California Civil Procedure Code.

<sup>110</sup> § 2029.300.

<sup>111</sup> § 2029.300 (a), stating “[a] request for the issuance of a subpoena under this section does not constitute making an appearance in the courts of this state.”

<sup>112</sup> § 2029.600.

<sup>113</sup> § 2029.700(a) provides that the Act “may be referred to as the «California version of the Uniform Interstate Depositions and Discovery Act».”

<sup>114</sup> Prefatory Note and Comments (2008), p. 6.

<sup>115</sup> § 2029.200 provides in the relevant part:

In this article:

(a) “Foreign jurisdiction” means either of the following:

(1) A state other than this state.

(2) A foreign nation.

<sup>116</sup> *Supra* (note 84).



anonymously exercise freedom of expression.<sup>117</sup> Furthermore, it seems unclear whether this Act is also applicable to a foreign judgment ordering disclosure which is based on a substantive (non-procedural) right such as the right created by the Japanese Act.<sup>118</sup> The Act is applicable to a foreign “subpoena,” which may be taken as implying that the Act is an instrument of cross-border judicial assistance rather than an instrument for the enforcement of foreign judgments. If so, it may not cover foreign judgments based on a substantive right.<sup>119</sup> On the other hand, the Act defines the word “subpoena” by referring to a “document, however denominated,”<sup>120</sup> which lends support for a broad interpretation.

## VIII. Conclusions

The foregoing analysis has revealed various approaches to unmasking anonymous online authors. Those approaches are still evolving, as apparent from the fact that almost all cases examined in the present article were decided within the past ten years. But it seems worth comparing and contrasting those diverse approaches at this stage of development to consider their implications for the questions related to conflict of laws which may arise in international contexts.

A disclosure order is based on a substantive right under Japanese law. It is presumably so under the French Trust in Digital Economy Act. Accordingly, both choice-of-law and jurisdictional questions are raised. With respect to choice of law, the question arises whether the claim should be characterized as tort or whether the right should be regarded as emanating from an overriding mandatory rule (*loi de police*). With respect to jurisdiction, if no jurisdictional ground similar to the Japanese version of “doing business” jurisdiction is available, it may be necessary to resort to the jurisdictional ground for tort claims, however awkward it may be, to

---

<sup>117</sup> F. CHAFIOL-CHAUMONT, *supra* (note 36), though not referring to the Californian Interstate and International Depositions and Discovery Act, cites the importance attached to the freedom of expression in the United States as a reason for stating her view that the enforceability of a French discovery order in California is uncertain.

<sup>118</sup> See *supra* (note 13).

<sup>119</sup> As regards the converse question of whether a procedural order for taking evidence is entitled to be enforced under an instrument for the enforcement of foreign judgments, a negative answer has been given by the CJEU in the context of what is now the Brussels I-bis Regulation in Case C-332/11, *ProRail v. Xpedys and others* [2013], para. 39.

<sup>120</sup> § 2029.200 provides in the relevant part:

In this article:

[...]

(e) “Subpoena” means a document, however denominated, issued under authority of a court of record requiring a person to do any of the following:

[...]

(2) Produce and permit inspection, copying, testing, or sampling of designated books, documents, records, electronically stored information, or tangible things in the possession, custody, or control of the person.

obtain jurisdiction over a foreign ISP. The enforcement of a disclosure order abroad would, to the extent that it is based on a substantive right, have to rely on the mechanism for the enforcement of foreign judgments.

In the United States, England and France, procedural disclosure orders are available.<sup>121</sup> As procedural orders, they are subject to the *lex fori* and raise no choice-of-law questions. On the other hand, jurisdictional questions do arise. In the United States, the debate is focused on personal jurisdiction over a suit against the anonymous author whereas in England, personal jurisdiction over a suit against the ISPs featured in a few cases. Either way, the jurisdictional analysis is not straightforward. In the United States, the difficulty arises from the anonymity of the defendant author. In England, the difficulty relates to finding bases of jurisdiction for a claim having no cause of action. Besides the question of personal jurisdiction, the question of jurisdiction to prescribe arises. While courts may make extra-territorial disclosure orders (as discussed above in the context of the French and English orders), the enforcement of such orders with coercive measures could infringe the sovereignty of other States. Being procedural orders, their enforcement abroad would have to rely on the mechanism for cross-border judicial assistance as available under international instruments (*e.g.* Hague Evidence Convention) or the domestic law of the requested State (*e.g.* Californian Interstate and International Depositions and Discovery Act).

When the identity of an anonymous online author is sought to be revealed, the stake of the author is greater than that of ISPs.<sup>122</sup> The author may wish to resist disclosure by relying on the applicable substantive threshold for disclosure,<sup>123</sup> maintaining, for example, the factual correctness of the material posted or their belief in it. Since the ISPs do not have such information, they cannot adequately represent the author's interest nor do they have inherent interest in protecting the latter. It would, therefore, seem necessary to protect the interest of anonymous authors not only by setting a substantive threshold for disclosure, but also by giving them procedural, including jurisdictional, safeguards. To achieve this goal while at the same time opening an avenue for relief for the injured person, a legal scheme consisting of the following elements seems ideal:

- (1) allow a suit to be filed against an anonymous author;
- (2) allow a procedural disclosure order of, if necessary, extra-territorial scope to be made against the ISPs;
- (3) require jurisdiction over a claim against the anonymous author to be established at least on a *prima facie* basis, so that the injured person, as the plaintiff, can show a good faith belief that the disclosure would conclusively establish the jurisdiction;

---

<sup>121</sup> The Japanese Code of Civil Procedure contains provisions for the collection of evidence prior to filing a suit (Ch. VI of Part I of the Code). But they are not available unless an advance notice of the filing of a suit has been given to the putative defendant. Accordingly, they are unhelpful where the identity of the putative defendant is unknown.

<sup>122</sup> As discussed under section II. above.

<sup>123</sup> See *supra* (note 8).

- (4) require the plaintiff and the ISPs to notify, to the extent possible, the anonymous author of the application for disclosure and allow the latter to contest the jurisdiction as well as other prerequisites for disclosure without revealing his or her identity;
- (5) allow a foreign disclosure order to be enforced with a light-touch review of jurisdiction and procedure; and,
- (6) exempt ISPs from liability towards the author for the breach of their duty of confidentiality provided that they have complied in good faith with a disclosure order or an enforcement decision thereof.

Some comments on each of these elements seem due. With respect to Element (1), while it is possible to bring suits against unnamed defendants in England and the United States, it is not universally so.<sup>124</sup> If a suit cannot be filed against an anonymous author, it may be necessary to take the cumbersome step of instituting two separate proceedings to make two claims for disclosure: the first against the host of the server or website (② in FIGURE above) and the second against the internet access provider (③ in FIGURE above). If the author is not party to the proceedings, the ISPs may not be able to adequately represent his or her interest.

With respect to Element (2), it would not be necessary to make a substantive (non-procedural) right of disclosure available. A claim based on a substantive right, as available in Japanese law, could be made in and out of court. But there is little point in allowing an out-of-court claim for disclosure since the ISPs would invariably resist such a claim in order to avoid liability towards the author. A claim based on a substantive right would also give rise to a difficult choice-of-law question, which is not raised by a procedural disclosure order. The latter instead raises the question of jurisdiction to prescribe. It is often necessary to make an order of extra-territorial scope but it would not violate the sovereignty of other states unless a coercive measure of enforcement is additionally taken.<sup>125</sup>

Element (3) is necessary to give the author jurisdictional protection, allowing him or her to oppose disclosure in a forum which would have jurisdiction over substantive proceedings. It must be admitted that where the defendant's identity is unknown, a complete jurisdictional inquiry is not possible. Thus, while the defendant's place of domicile or habitual residence is a ground of jurisdiction in many

---

<sup>124</sup> Thus, in Japan, the civil procedure rules generally do not allow an unnamed defendant to be sued. Art. 133(2) of the Japanese Code of Civil Procedure provides in the relevant part (the present author's translation):

“A claim form shall state the following matters:

(i) the parties and their statutory agents;” [...]

It has been discussed whether to introduce the John Doe type suits for the cases of anonymous online authors but has been concluded to be difficult since it would have far-reaching implications for all aspects of civil procedure from the commencement of suit to the effect of judgments: WORKING GROUP ON THE REVIEW OF THE ACT ON THE LIMITATION OF LIABILITY OF THE PROVIDERS OF SPECIFIED TELECOMMUNICATION SERVICES, *Recommendation of the Working Group on the Review of the Act on the Limitation of Liability of the Providers of Specified Telecommunication Services* (2011), p. 40 (in Japanese).

<sup>125</sup> See *supra* (note 104).

states, it will often be impossible to ascertain (or even guess) where such places are situated if the defendant is anonymous. Jurisdiction may, however, be founded under the *loci damni* rule on the basis of accessibility of the offending online content in the forum state<sup>126</sup> or under the *loci actus* rule by way of geolocation of the IP address (where known to the plaintiff) used to post the content.<sup>127</sup> Again, where the law requires an overall assessment of factual circumstances, as does the US minimum contacts test, a full-fledged jurisdictional inquiry is not possible. It should, therefore, be considered to be sufficient to establish jurisdiction on a *prima facie* basis, a low threshold test which can be satisfied by showing a good faith belief that the disclosure would conclusively establish the jurisdiction.<sup>128</sup>

Element (4) is necessary to give, to the extent possible, the author an opportunity to anonymously oppose the application for disclosure. As seen above, while in the United States, the plaintiffs are generally required to make efforts to notify the anonymous author of their claim,<sup>129</sup> Japanese law makes it mandatory for the ISP, from whom disclosure is sought, to consult with the author unless the latter cannot be contacted.<sup>130</sup> Among the different types of ISPs, the administrator of the website used by the author may only know the IP address used, whereas the internet access provider is more likely to be able to contact the author. It would be possible for the author to oppose disclosure without revealing his or her identity by, for example, submitting a written response or retaining counsel.

Element (5) would be useful since the ISPs may not be willing to comply with a disclosure order unless it is recognised or enforced in the states, such as their home state or the state in which they store the information sought, where a suit is likely to be brought to pursue their liability towards the author for breach of their duties of confidentiality. While the simplicity of the Californian Act for the enforcement of foreign subpoenas is attractive, an express provision on jurisdictional and procedural review would be helpful to improve clarity. The review should have a light touch because a full-fledged jurisdictional inquiry is not possible while the defendant author is anonymous and because notice to the author cannot always be given.

Element (6) would be useful to avoid double jeopardy for the ISPs. To come up with a suitable expression for good faith compliance, the Privacy policy statement of some ISPs<sup>131</sup> may offer helpful guidance.

---

<sup>126</sup> See *supra* (note 41).

<sup>127</sup> See the text reproduced *supra* note 68.

<sup>128</sup> See the text reproduced *supra* note 61 for a ruling applying a similar test.

<sup>129</sup> See *supra* (note 65).

<sup>130</sup> See *supra* (note 12).

<sup>131</sup> See *supra* (note 98) for an example.