The Intersection Between Data Protection and Trademark Rights: Balancing Fundamental Rights

By Ruth Hoy and Jeremy Blum

1. Data Protection Regime in the EU

Both the right to the protection of intellectual property[1] and the right to protection of personal data[2] are protected as fundamental freedoms of the European Union. The purpose of this article is to analyse how those competing rights have been balanced in the context of trade mark enforcement, in particular whether rights or obligations to protect personal data have been used to interfere with the enforcement of trade marks within Europe. The discussion herein will generally consider circumstances in the course of trade mark enforcement where the disclosure of information may give rise to data protection concerns and whether such concerns have been utilised by data controllers or data subjects to block enforcement attempts.

Before engaging in any specific analysis, it is necessary to briefly outline the data protection regime at national and European level. The Data Protection Directive[3] sets out the basic legislative framework in Europe for the protection of personal data. By way of example, the Directive has largely been transposed into English law by the Data Protection Act 1998 ("DPA 1998"). The obligations under the DPA 1998 fall on the "data controller" as the person who determines the purpose for obtaining personal data and the manner in which it is processed. The DPA 1998 also confers certain rights on "data subjects" who are the individuals about whom personal data is processed. "Personal data" is defined as any information relating to an identified or identifiable natural person. In an online context, the definition of personal data extends to static IP addresses because they allow users to be identified.[4]

The DPA 1998 places an obligation on data controllers to ensure the fair and lawful processing of personal data.[5] Processing is only considered fair if one of a number of criteria are met, e.g. the disclosure of information is done with the consent of the data subject or is necessary to comply with a legal obligation. For present purposes, the most relevant exemption is that personal data is exempt from non-disclosure if disclosure is required by order of a court[6], is necessary for the purpose of or connection with legal proceedings, obtaining legal advice or for the purpose of establishing, exercising or defending a legal right.[7]

It is important to note that in certain EU Member States, the conflict discussed herein between the right to the protection of intellectual property and the right to protection of personal data is, in fact, very

[1] European Charter of Fundamental Rights, Article 17.2.
[2] European Charter of Fundamental Rights, Article 8.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[4] Case C-70/10 *Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)* [2012] E.C.D.R 4. Further, in France, the *Cour de cassation* (i.e. the highest court in the French legal system) recently confirmed that IP addresses, as they indirectly allow a person's identification, are personal data (see decision n° 15-22.595 dated 3 November 2016), thereby putting an end to a 15-year long doctrinal and judicial debate as to the nature of IP addresses, and finally aligning French case-law with the position of the French Data Protection Authority (CNIL), the French *Conseil Constitutionnel*, and the Court of Justice of the European Union ("CJEU") (as recently reaffirmed in Case C-528/14, dated 19 October 2016). See also recital 30 of the recent European Regulation on Data Protection 2016/769, which will come into force on 25 May 2018, stating that IP addresses are in essence personal data covered by the Regulation; "*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*" (emphasis added).
[5] Schedule 1 Data Protection Act 1998
[6] Data Protection Act 1998, Section 35(1)(c)
[7] Data Protection Act 1998, Section 35(2)

limited. For Spain, the reason for the lack of tension is the way in which its national laws interact. The Spanish Data Protection Act LO 15/1999 ("LOPD") is one of the most stringent legal frameworks for data protection within the EU, with enforcement by the Spanish Data Protection Commissioner acknowledged as zealous and strict, however conflict between privacy rights and intellectual property rights is rare. The LOPD provides that where personal information is requested pursuant to an Act of Parliament or some other legal provision of the same status, the protections afforded by the LOPD cease to apply.[8] Additionally, the LOPD does not offer protection of personal data where such information is intended for a judge, public prosecutor, ombudsman, or the Court of Public Accounts in charge of the relevant case.[9] As trademarks are regulated by an Act of Parliament and disputes are managed by the courts of justice, tension does not arise. Although such exceptions may appear to undermine a paramount constitutional right, any request for disclosure of personal information that does not fall under the exceptions can be successfully resisted, such as an obligation to disclose contained in a regulation or attempts by the police to procure such information without a court order or other special legal entitlement. As the *Promusicae* case shows (below), this does not avoid conflicts that may appear from time to time.

2. The right to information

a) Article 8 Enforcement Directive

Article 8(1) of Directive 2004/48 (Enforcement Directive)[10] requires Member States to ensure that in litigation proceedings concerning the infringement of intellectual property, a national court may order for the disclosure of information regarding the origin and distribution network of infringing goods to be provided by the infringer or any person in possession of infringing goods, found to be using or providing infringing services on a commercial scale, or involved in the production, manufacture or distribution of infringing goods or services.

Although Article 8 will be considered generally in the context of this article, the way in which it has been transposed into national laws varies across different Member States. By way of example, in Poland,[11] one is entitled to request for the disclosure of personal information in the context of alleged intellectual property infringement before formal proceedings have commenced.[12] Further, the data that may be requested under Polish law is broad, including data which is possibly not relevant to the claim or data which relates to a separate individual who is not the data subject.[13] As such, there is no requirement, in Poland, to establish a connection between the request for disclosure of personal data and the initiation of formal proceedings. Therefore, the Polish laws on the right to information represents a framework that differs significantly from the Enforcement Directive and the original intentions of the European draftsmen. This has led to some confusion in the national courts, with some judges adopting a pro-European interpretation of the national law and only giving an order for the disclosure of information should formal proceedings be issued.

The very nature of the disclosure under Art 8(1) unearths a tension between enforcement of intellectual property rights on the one hand and protection of confidential information and privacy on the other. This tension is envisaged by Art 8(3)(e) which provides that Art 8(1) applies without prejudice to the protection of confidential information and data protection, which is interpreted as a general obligation

[8] LOPD Article 11.2(a)
[9] LOPD Article 11.2(d)
[10] Directive 2004/48 on the Enforcement of Intellectual Property Rights
[11] Article 8 of the Enforcement Directive was transposed into the national law of Poland in the Industrial Property Act of 30 June 2000, particularly Article 286^1 (securing the claims and right to information)
[12] Article 286^1 states that the court also before the action is brought examines the motion of the right holder to secure claims by obligating an infringing party or a different person than the infringing party to provide information, which is required to pursue the claims.
[13] Contrary to Article 8 of the Enforcement Directive, Article 286^1 of the Industrial Property Act does not require that the request of the claimant for the disclosure of information should be justified and proportionate.

to consider the proportionality of remedies for the infringement of intellectual property rights, including orders for the disclosure of the identities of infringers.[14]

A further illustration of how EU Member States have interpreted and transposed Article 8 of the Enforcement Directive is provided by the French IP Civil Code,[15] and the corresponding provision to Article 8(3)(e), which makes no reference to "confidential information" or "personal data" but rather makes the right of information subject to, more generally, the absence of any "legitimate impediment" to doing so. There is little guidance provided by the case law on whether the protection of confidential information or personal data would be considered to be a "legitimate impediment" in the context of trade mark infringement and this therefore provides no further clarity on the inherent tension between 8(1) and 8(3)(e).[16]

In accordance with Art. 8(1) of the Enforcement Directive, the German legislature has implemented broad and widely uniform disclosure claims for rights holders in cases of IP violations. These disclosure claims have been implemented in the most relevant IP areas of patents, trademarks, designs and utility models and the wording of Art 8(1)(a)-(d) has largely been adopted into domestic statutory law.[17] Under these provisions, rights holders of national IP rights, as well as of a EU trade mark or European patent with designation of protection for Germany, are given a strong set of remedies to obtain relevant information on the infringement suffered. The material threshold to be overcome by the rights holder in his quest for information is the statutory requirement of "obvious violation of a protected right" that is common to all disclosure provisions transposed into German IP rights statutes from the Enforcement Directive. This imposes both an initial evidential hurdle on the plaintiff rights holder and a proportionality restriction that effectively subjects the disclosure claim to some sort of severity degree. From a practical viewpoint, however, this restriction is of virtually no relevance in cases regarding counterfeit activities, file sharing systems or pirated content platforms/networks, as infringement activities occurring under these circumstances usually constitute obvious violations. The same fate similarly befalls data protection interests of infringers, as statutory law is clear, with little discretion for German courts to balance the privacy interests of the data subjects against the rights holders demand for disclosure. If the requirements of the disclosure claim under statutory law have been shown and substantiated, the order is to be granted as per the plaintiff rights holder's request and in accordance with the relevant statutory provisions determining its scope.[18] Consequently, German courts tend to accord little to no weight to data protection considerations in their respective findings. Material data protection concerns may only arise in very specific infringement cases where the defendant sued and the data subject targeted by the disclosure order are not the same person. Court cases dealing with this kind of scenario are generally characterised through a well-known triangular relationship: the plaintiff rights holder suing an intermediary service provider where a third party is taking advantage of the defendant intermediary's services for the purpose of committing immediate acts of IP rights infringement. In all the cases that came before the German courts, however, data protection concerns were neither a significant issue nor a notable side consideration, with the material issues centring on the criteria and scope of intermediary liability, as well as the prerequisite showing and degree of

[14] Case C-324/09 *L'Oréal SA v eBay International AG* [2011] ECR I-0000 at [139]-[144]

[15] Transposition of Art. 8 of the Enforcement Directive into French law was made through Statute n° 2007-1544 of 29 October 2007, which created a new Art. L. 716-7-1

[16] It is worth noting that "legitimate impediment" is a broad, blurry notion, also present in art. 11 § 2 of the French Code of Civil Procedure, which allows a judge to order a third party to produce documents in its possession, save for where there is a "legitimate impediment" to doing so. However, according to case-law, the judge's power under this article shall be limited only by "*the existence of a legitimate impediment involving either the respect of privacy –except if the measure requested is necessary to protect the rights and freedoms of others– or professional secrecy*" (see French *Cour de cassation* n° 85-16.436, dated 21 July 1987)

[17] Section 19 of the German Trademark Act, Section 140b of the German Patent Act, Section 24b of the German Act on Utility Models, Section 46 of the German Design Act, Section 37b of the Plant Varieties Protection Act.

[18] *ibid.*

substantiation required by the plaintiff to enable enforcement of his IP rights through the infringement claims.[19]

Judicature of the CJEU

The scope of the Article 8 obligation was considered in the *Promusicae*[20] decision. The CJEU confirmed that an application for the disclosure of personal data pursuant to the enforcement of property rights falls squarely within the scope of Art 8.[21] After considering, inter alia, the obligations under Directive 2002/58[22], the CJEU concluded that Article 8(1), read in light of para (3)(e), does not require Member States to lay down an obligation to communicate personal data.[23] In reaching that decision, the CJEU also recognised that the situation *obliged the national court* to reconcile the protection of conflicting fundamental rights and reiterated that the transposition of provisions into national law requires an interpretation that strikes a fair balance between fundamental rights and conforms to general principles of Community law.[24]

In *Bonnier*,[25] the CJEU considered the applicability of Art 8 in the context of Directive 2006/24/EC[26] in the context of copyright infringement by means of an FTP server that allowed files to be shared and data to be transferred via the Internet.[27] The applicant sought the name and address of the user of the IP address from which the infringing files were shared; the relief sought under Art 8 was opposed on the grounds that the disclosure of such information was contrary to Directive 2006/24.[28] The CJEU held that Directive 2006/24 did not preclude an application of the kind sought, but that national courts needed to ensure an interpretation of the law that allowed them to strike a fair balance between the fundamental rights and freedoms concerned.[29]

More recently, in relation to trade mark infringement, the CJEU in *Coty*,[30] considered whether relief under Article 8 was precluded by a provision of German banking law. At national level, the Oberlandesgericht Naumburg held that although banking services had been used to facilitate infringement, the Stadtsparkasse was entitled, under Paragraph 383(1) of the Civil Procedure Code, to refuse to give evidence in civil proceedings. The Bundesgerichtshof referred the matter to the CJEU who determined that the unqualified nature of the provision of national law was liable to frustrate the application of Article 8(1) and thereby seriously impair the effective exercise of the fundamental right to property.[31] The Court of Justice was clear in concluding that a provision of such unlimited and unqualified character was precluded, by virtue of Article 8(3)(e), from preventing the disclosure of personal data under Article 8(1).

The decisions in *Bonnier* and *Coty* illustrate how rights to the protection of personal data could be used to frustrate enforcement actions. In *Coty*, taken by itself, the unqualified banking law, by its very nature had the potential to entirely undermine the object of Article 8(1). In order to strike a fair balance between

---

[19] See recent decisions of Federal Court of Justice, inter alia: rulings of 26 November 2015, docket no. I ZR 174/14 - *Goldesel*, and docket no. I ZR 3/14 - *Deutsche Telekom*; ruling of 19 April 2012, docket no. I ZB 80/11 - *Alles kann besser werden*.
[20] *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU (C-275/06)* [2008] 2 C.M.L.R. 17
[21] [2008] 2 C.M.L.R. 17 [58]
[22] ePrivacy Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector
[23] [2008] 2 C.M.L.R. 17 [54]
[24] [2008] 2 C.M.L.R. 17 [70]
[25] Case C-461/10 *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] 2 C.M.L.R. 42
[26] Data Retention Directive 2006/24/EC and amending Directive 2002/58
[27] [2012] 2 C.M.L.R. 42 [26]
[28] [2012] 2 C.M.L.R. 42 [51]-[52]
[29] [2012] 2 C.M.L.R. 42 [54]
[30] Case C-580/13 *Coty Germany GmbH v Stadtsparkasse Magdeburg* [2015] 1 W.L.R. 4283
[31] 1 W.L.R. 4283, [39]-[40]

the competing rights, the protection of personal data had to yield to the right of protection under Article 8. Whilst the decision in *Coty* favours IP enforcement, the rationale and decision is hardly revolutionary. The inherent character of an unqualified privacy right precludes a court from balancing competing rights to achieve a proportionate solution.

The jurisprudence of the CJEU confirms that the right to information is designed to apply and implement the fundamental right to an effective remedy guaranteed in Article 47 of the Charter, thereby ensuring the exercise of the fundamental right to property, but that in doing so the protection of intellectual property should not hamper, inter alia, the protection of personal data.[32]

b) Norwich Pharmacal Orders

Arguably the best illustration of how the courts approach the ultimate balancing act comes at national level. The Norwich Pharmacal Order ("NPO") is not a product of the 21st Century, nor is it a weapon the court has created to combat online infringement; nevertheless the remedy emanated from the context of IP enforcement in *Norwich Pharmacal Co v Customs and Excise Commissioners*.[33] Since then, a substantial body of jurisprudence has sculpted the conditions for relief, with the most relevant for present purposes being that the disclosure sought must be proportionate.[34] The existence of the Norwich Pharmacal doctrine was the very reason Article 8 was not transposed into English law.[35]

Norwich Pharmacal relief is generally used as a preparatory step that allows a proprietor to obtain information from an intermediary about, inter alia, the identity of the alleged infringer that a proprietor may otherwise not be able to obtain. The premise for the relief is that the intermediary has facilitated, albeit innocently, the commission of allegedly infringing acts and therefore is under an equitable duty to disclose.[36] It is an order originating in the UK but is also available in other common law countries.

In France, art. L. 716-7-1 of the IP Code, which transposed Article 8 of the Enforcement Directive, was successfully invoked by Hermès against eBay and one of its users in order to be provided with detailed information regarding the online sales of counterfeit Hermès bags. In this case, eBay France failed to rely on the French transposition of article 8(3)(e) (i.e. the last paragraph of article L. 716-7-1), as they failed to convince the Court that there existed a "legitimate impediment" for eBay France to disclose the personal data requested. On the contrary, the Court considered that eBay France was both legally and technically in a position to provide the requested information (notably because eBay France had filed in its own name a personal data processing declaration to the French DPA). As a consequence, eBay France and eBay International AG were ordered to provide specific information. The information was, however, limited to the sellers and buyers of the counterfeit bags, as according to the Court, eBay was "*obviously not in the possession of other information on producers, manufacturers and distributers of the bags*" (eBay and the user were therefore only ordered to produce information such as names and addresses of the sellers and buyers of the counterfeit bags, the number of sales and the prices, and the exchanges of emails between sellers and buyers)[37].

It is worth noting that, unlike with the NPO, the right to information can only be used, under French law, when a court is already seized of a dispute. Indeed, where NPO is generally used as a preparatory step, the French right to information suggests that a request be made to "*the jurisdiction seized on the merits or pre-trial*".

---

[32] 1 W.L.R. 4283, [29]-[32]
[33] [1974] AC 133, 175B-C, per Lord Reid
[34] *Rugby Football Union v Consolidated Information Services Limited (formerly Viagogo Limited)* [2012] UKSC 55
[35] The Intellectual Property (Enforcement, etc.) Regulations 2006, Explanatory Note, paragraph 1.
[36] [1974] AC 133
[37] Reims Court of appeals, 5 May 2009. The Court's decision was also due to the existence in French law of article 6-II, al. 3, of Statute n° 2004-575 of 21 June 2004 ("statute for the confidence in the digital economy"), which allows the judicial authority to request communication from hosting providers of data allowing to identify whoever took part in the creation/upload of a specific content on a service provided by the hosting providers.

Peppermint Jam v Telecom Italia (unreported), which was an Italian case filed in 2006, concerned a music company seeking disclosure from an ISP of the personal data of internet users involved in peer-to-peer sharing of audio-files online in breach of the claimant's copyright. At first instance, the Italian Court issued an order granting interim relief to Peppermint that obliged the ISP to provide the personal data requested, which related to over 3000 individuals. Unsurprisingly, this gave rise to criticism and consumer associations took action before the Italian Data Protection Authority. This led to the case being appealed and subsequently overturned on the grounds that the protection of personal data in electronic communications took priority over digital copyright enforcement undertaken through measures dependent upon the disclosure of unauthorised file-sharers. The Italian Data Protection Authority also issued an order against Peppermint requiring them to destroy all the personal data originally collected as it was not compliant with applicable data protection laws. This staunch protection of the personal data in this case is illustrative of the variable standards in regards to the balancing of fundamental rights, even within the context of NPO or similar orders for relief.

Contrary to the NPO doctrine, which is an equitable product of the judiciary and has been continuously shaped in case law, the disclosure remedy afforded under German law is primarily a result of the transposition of Art. 8(1) of the Enforcement Directive. Under the pertinent statutory provisions, the enforceability of the disclosure claim is likewise dependent on a contribution of the intermediary facilitating the IP infringing activities, namely (i) the provision of services on a commercial scale; and (ii) use for the infringing activities, as originally laid down in Art. 8(1)(d) of the Enforcement Directive. The plaintiff is entitled to the disclosure order if the court is persuaded on the basis of the plaintiff's showing that (i) an act of obvious IP infringement was committed to the detriment of the rights holder; and (ii) the defendant intermediary made the aforementioned contribution to this act of infringement. With regard to scope of information that may be claimed by the plaintiff, the disclosure remedies incorporated into German statutory law fully conform to Art. 8(2) of the Enforcement Directive. In this context, a recent first instance court ruling on the scope of the disclosure claim under the German Copyright Act has expressly clarified that the disclosure order does not extend to the data subjects contact information, namely e-mail address, telephone number and the date and time the IP address was recorded.[38]

Moreover, statutory law provides for one important restriction to the disclosure of personal data of the immediate infringer: if the disclosure of the requested personal data is contingent on the use or evaluation of so-called "traffic data", such disclosure is subject to a prior court order expressly declaring the use of the traffic data to be permissible.[39] This statutory restriction is of particular relevance in cases where the plaintiff seeks to obtain disclosure of the internet user's name and postal address assigned to a dynamic IP address that was allocated to the internet user for a session at a specific time and date. While the name and address of the targeted internet user are not considered to be "traffic data" under German and EU case law, the dynamic IP address is undoubtedly qualified as traffic data, which therefore triggers the statutory requirement of a judicial clearance order.[40]

As with the Art 8 jurisdiction, the nature of disclosure under a NPO invokes a direct conflict between data protection and IP enforcement, as Arnold J surmised, '*The grant of the order sought will invade their privacy and impinge upon their data protection rights'*.[41] Our concern is whether those rights have

[38] Regional Court of Frankfurt am Main, ruling of 3 May 2016, docket no. 2-03 O 476/16.

[39] German Federal Court of Justice, ruling of 19 April 2012, docket no. I ZB 80/11 - "Alles kann besser werden" - Recital 37 et seq.
"Traffic data" is defined by Section 3 No. 30 of the German Telecommunications Act as data that is collected, processed and used in connection with providing telecommunication services. This definition comprises all such data containing information on communication activities that occurred from certain access points between certain users at a specific time and for a specific duration.

[40] see under Footnote 39, Recital 39 et seq.

[41] *Golden Eye (International) Limited v Telefonica UK Limited* [2012] EWHC 723, [119]

been utilised to frustrate the enforcement of intellectual property rights. Undoubtedly, in exercising their jurisdiction the courts have recognised the importance of data protection and privacy concerns.

As Aldous LJ observed in *Totalise plc v Motley Fool Ltd*:

'…no order is to be made for disclosure of a data subject's identity, whether under the Norwich Pharmacal doctrine or otherwise, unless the court has first considered whether the disclosure is warranted having regard to the rights and freedoms or the legitimate interests of the data subject". [42]

However, courts have been equally concerned to ensure privacy does not frustrate effective enforcement. In the Irish High Court, Charleton J observed:

"*Criminals leave the private sphere when they infringe the rights of others or conspire in that respect".* [43]

In a later *EMI* decision[44], Charleton J was once again robust in dismissing arguments of privacy as a barrier to enforcement in mass copyright infringement. The judge concluded that participation in peer-to-peer lending platforms did not legitimately carry the expectation of privacy. Consequently, even though the injunction would impinge on users' right to protection of personal data, the measures taken to enforce rights of the proprietors were proportionate.[45]

In *Golden Eye*, the application concerned the disclosure of the names and addresses of customers alleged to have committed copyright infringement by means of a peer-to-peer lending platform.[46] At first instance, Arnold J engaged in a detailed assessment of the Norwich Pharmacal doctrine. Arnold J recognised that the order would impinge on the end users' data protection rights and privacy.[47] Whilst Arnold J granted an order for disclosure in favour of Golden Eye and a second claimant, his decision in relation to the other claimants was heavily influenced by the litigation agreement they had with Golden, which in his opinion would be tantamount to the court sanctioning the sale of the intended defendants' privacy and data protection rights to the highest bidder.[48]

On Appeal, the Court of Appeal appeared to endorse Arnold's overall application of the Norwich Pharmacal jurisprudence, however disagreed with Arnold J on the impact of the litigation agreement, to the extent that the data protection and privacy of the end users were insufficient to prevent the Court from granting a Norwich Pharmacal Order in favour of all claimants.[49]

Interestingly, in the majority of cases the respondents do not contest the order sought and those most affected, the end users, are not present. As Lord Justice Aldous opined:

"It is difficult to see how the court can carry out this task if what it is refereeing is a contest between two parties, neither of whom is the person most concerned, the data subject; one of whom is the data subject's prospective antagonist; and the other of whom knows the data subject's identity, has

---

[42] [2001] EWCA Civ 1897, [24]

[43] *EMI Records (Ireland) ltd v UPC Communications (Ireland) Ltd* [2010] IEHC 377, at [68]. See also CJEU Case C-324/09 *L'Oréal SA v eBay International AG* [2011] at [142] which states *"in order to ensure that there is a right to an effective remedy against persons who have used an online service to infringe intellectual property rights, the operator of an online marketplace may be ordered to take measures to make it easier to identify its customer-sellers. In that regard, as L'Oréal has rightly submitted in its written observations and as follows from Article 6 of Directive 2000/31, although it is certainly necessary to respect the protection of personal data, the fact remains that when the infringer is operating in the course of trade and not in a private matter, that person must be clearly identifiable"* [emphasis added].

[44] *EMI Records (Ireland) Ltd v Data Protection Commissioner* [2012] IEHC 264

[45] [2012] IEHC 264, 284

[46] [2012] EWHC 723

[47] [2012] EWHC 723, [119]

[48] [2012] EWHC 723, [146]

[49] *Golden Eye (International) Ltd and others v Telefónica UK Ltd and another* [2012] EWCA Civ 1740

undertaken to keep it confidential so far as the law permits, and would like to get out of the cross-fire as rapidly and as cheaply as possible".[50]

In one of the few trade mark decisions on this topic, the application in *Wilko Retail Ltd v Buyology Ltd*[51] concerned disclosure of the details of the supplier of counterfeit products alleged to infringe the applicant's trade mark. Even though Buyology did not oppose the order sought, the court refused to grant the order on the basis that there was no evidence of any further irreparable harm to Wilko's business and therefore the irreparable harm caused to Buyology by granting the order outweighed the benefit of granting the order.[52] In *Football Association Premier League Ltd v Wells*[53], Snowden J, in the absence of the defendant, granted an order for disclosure of the names and address of those responsible for providing the equipment that allowed the defendants to stream Premier League football matches in breach of FAPL rights.

In contrast, the interests of the end user were to a degree represented in the *Golden Eye* dispute. The consumer rights group, Consumer Focus, was joined to the litigation to represent the interests of end users and this allowed qualifications to be applied to the proposed order.[54] However, this level of representation is the exception rather than the rule. Highlighting the absence of the data subject in such proceedings is not to criticise the court for failing to effectively ensure respect for data protection and privacy rights, rather it is to illustrate that, in the context of NPO, privacy and data protection rights are not being used as a weapon to frustrate infringement actions. In many cases the approach of the data controller is one of damage limitation, hence why many of the orders are not disputed on privacy grounds.

In an online context, the prevalence of data protection and privacy concerns raise important distinctions between the nature of online copyright and trade mark infringement. Particularly in peer-to-peer lending cases, the scope for infringement is incredibly vast given the act of accessing and downloading the copyright material. On the other hand, an end user who innocently purchases a counterfeit product via an infringing website or platform does not infringe, and thus a sea of end users is not necessarily the target of an NPO in a trade mark context. Accordingly, the need to identify users on a mass scale is unlikely in a trade mark context, the corollary being that data protection and privacy issues might be less prominent.

3. The limitations on disclosure and Discovery

The previous discussion centred on the data protection issues arising from orders for injunctive relief under Article 8 and through the Norwich Pharmacal doctrine. Typically, Norwich Pharmacal relief is sought from an innocent third party that has become mixed up in facilitating infringement, thereby triggering an equitable duty to disclose the identity of the alleged infringer.[55]

Such cases can be distinguished from cases in which disclosure of personal data is sought from the defendant in an infringement action, in order to substantiate the claims against them. In those circumstances, the defendant's interest in seeking to frustrate any such request is axiomatic, the corollary being that there is greater scope for issues of data protection to be used as a sword to wound infringement claims.

Consequently, the following section proceeds to focus on issues that may arise where disclosure is requested directly from a defendant to proceedings. The DPA 1998 anticipates that the disclosure of

[50] [2001] EWCA Civ 1897 at [26]
[51] [2015] E.T.M.R. 13
[52] [2015] E.T.M.R. 13 [25]-[29]
[53] [2015] EWHC 3910
[54] [2012] EWHC 723, [7]-[9]
[55] [2015] EWHC 3910, per Snowden J at [7]

personal data is justified in certain circumstances. Section 35(2) provides that such circumstances include disclosure for the purpose of obtaining legal advice, establishing, exercising or defending legal rights or in connection with any legal proceedings.

The ICO[56] suggests that organisations may find it difficult to determine if disclosure is necessary, and therefore a data controller may refuse to comply with the request. If that approach is taken, a proprietor seeking to enforce their rights could face the additional hurdle of obtaining a court order simply to evaluate the strength of their claim.

In *Interflora v Marks and Spencer plc*,[57] Interflora made an application for specific disclosure of a list of customers who on the same occasion used the Google search engine, searched using search term 'Interflora', clicked on a sponsored link for Marks & Spencer and purchased flowers from Marks & Spencer as a result of that search. In associated proceedings for trade mark infringement, *Interflora* asserted that Mark and Spencer's use of variations of the word 'Interflora' as part of their keyword advertising policy infringed their trade mark.[58]

Interflora made the request to identify customer information with a view to contacting those customers identified and determining if those customers were confused by Marks and Spencer's keyword advertising material. In opposition, Marks and Spencer asserted, inter alia, that the customers whose details would be disclosed under the order, had a legitimate concern in ensuring their personal information and privacy is respected. In dismissing the application, Arnold J recognised that the customers had provided their personal information for particular purposes, more specifically not for the purpose of enabling an opposition party to contact them for a source of evidence in litigation.[59] Furthermore, the continual need to monitor the proposed Interflora investigation to ensure respect for privacy and data protection also weighed heavily in Justice Arnold's decision.[60]

Evidently, the *Interflora* decision demonstrates how data protection and privacy may pose a barrier to IP enforcement, in the sense that information comprised of personal data can be withheld on data protection grounds because the mere prospect of infringement does not merit interference with the data subject's rights. A brand owner litigant may struggle to obtain relevant information if personal data is involved. It would appear that, post *Interflora*, an advertiser has legitimate grounds to reject an application for information on data protection grounds and force a proprietor to seek a court order. Limiting access to information regarding consumer habits has potential to interfere with an infringement claim by restricting the ability of the proprietor to substantiate an assertion of actual confusion.

That said, the decision to dismiss the application in *Interflora* was not solely based on data protection grounds. Arnold J recognised that aside from the privacy interests of the consumer, both the commercial interest of Marks & Spencer and the sheer scale of the proposed investigation justified dismissing the application.[61] It remains to be seen whether a similar application would be refused solely on data protection grounds. Arguably, the collective weight of the relevant factors provided sufficient grounds to dismiss the application, but the *Interflora* decision represents, at best, a procedural hurdle and, at worst, a potential barrier to evidence.

In the online environment keyword advertising has become a point of contention in the trade mark sphere as the courts attempt to delineate the powers of trade mark proprietors to restrict potentially infringing advertising activity.[62] The decision in *Interflora* could become the unintended prelude for

[56] Information Commissioners Office – www.ico.org.uk
[57] [2013] EWHC 270, per Arnold J [1]
[58] [2013] EWHC 1291
[59] [2013] EWHC 270, per Arnold J [12]
[60] [2013] EWHC 270, per Arnold J [18]
[61] [2013] EWHC 270 [17]
[62] C O'Doherty *'Online trade mark and copyright infringement injunctions: implications on ISPs, site owners and IPR owners'* (2016) 22(3) C.T.L.R 79

data protection rights to be used as a shield against putative trade mark infringement claims. The issue of keyword advertising is certainly not a fresh concern to the online environment, as early as 2004,[63] however with online advertising as prevalent as ever, it is submitted that the decision in *Interflora* may open the door for data protection to be used as a shield against infringement proceedings.

The Irish case of *Glaxo Group Limited & Ors v Rowex Limited*,[64] concerned discovery applications relating to, inter alia, a trade mark infringement claim. The subject of the dispute was the Seretide inhaler, which was hailed as a blockbuster product in the pharmaceuticals industry and one which Glaxo claimed they had invested significant time, effort and money into developing its goodwill and reputation, particularly its purple colour that was protected as a trade mark. Rowex was the Irish distributor for the Sandoz Group, which had produced its own inhaler that used a very similar shade of purple. The judgment addressed a number of issues including a concern as to the constraining effect of any German data protection laws with regard to any discovery that might be made by certain German entities not party to the proceedings. The judgment discusses the rules and principles relating to discovery, particularly in the context of corporate groups, at length. Within this discussion, the judge notes that *'the requirement that justice be administered fairly will trump any obligation of confidence in ordinary circumstances so that confidentiality will not, ordinarily, provide a basis for the non-disclosure of materials*',[65] whilst being mindful of the need to take a proportionate approach in order to sharpen the *'blunt tool of discovery'* and ensure that inappropriate disclosures of personal data are not authorised. The judge further commented that the principle of proportionality was particularly relevant where highly confidential documents were sought and where the relevance of such documents was marginal.[66] The judge also commented on the right of those individuals from whom disclosure of personal data was sought, stating that they would have the right to decline to consent to release of their personal data and that there is nothing the court could have done about that if such an election was made.[67]

Therefore, the decision in *GSK v Rowex* shows how data protection issues may be a stumbling block to the breath of discovery generally and in enforcement actions.

4. Blocking Injunctions

Article 11 of the Enforcement Directive provides a more general basis for relief stating that Member States must ensure that rights holders are able to apply for injunctive relief against intermediaries whose services are used to infringe an intellectual property right. Recital 59 of the Infosoc Directive[68] makes clear that in the digital environment the service of intermediaries may increasingly be used to infringe intellectual property rights, therefore in many cases those intermediaries are best placed to. Consequently, the blocking injunction has become a key weapon used in the battle of online infringement, particularly in the context of copyright infringement. In the copyright sphere, the jurisdiction for such relief has specific legislative basis in Europe under Article 8(3) of the Infosoc Directive, which is transposed into UK national law by Section 97A of the Copyright, Designs and Patents Act 1988.

Unlike Article 8(3) of the Infosoc Directive, Article 11 of the Enforcement Directive was not directly transposed into UK law, and it was unclear whether there was a legal basis for blocking injunctions in

[63] *Reed Executive plc and another v Reed Business Information and others* [2004] EWCA Civ 159. However, on appeal, the Court of Appeal held that there was no trade mark infringement for similar service marks.

[64] [2015] IEHC 368

[65] [2015] IEHC 368, [41]. It is noted that under EU law, *'individuals should enjoy a high level of protection when it comes to personal data*'.

[66] [2015] IEHC 368, [42]

[67] [2015] IEHC 368, [53]

[68] Directive 2001/29/EC of the European Parliament and of the Council of the of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

the context of trade mark infringement.[69] In the seminal UK High Court decision in *Cartier*,[70]Arnold J extended the jurisdiction for blocking injunctions to trade mark infringement. Kitchin LJ in the Court of Appeal has subsequently confirmed the availability of intermediary injunctions in trade mark cases.[71] Whilst the focus of this article is concerned with interplay between trade mark enforcement and data protection, the judgments of previous decisions in cases of copyright infringement will be illustrative of the approach taken by the English courts and EU courts.

In contrast with the Norwich Pharmacal Order, intermediary blocking injunctions do not inherently engage data protection and privacy rights. Consequently, in a number of decisions including *Twentieth Century Fox Film Corporation v Newzbin Limited (Newzbin 1)*[72] and *Twentieth Century Fox Film Corporation v British Telecommunications (Newzbin 2),*[73] data protection implications were not considered in granting intermediary injunctions. Rather, in *Newzbin 2*, it was submitted by BT that the blocking injunction engaged Article 10 ECHR and the relief sought was a disproportionate interference with the subscribers' rights. Arnold J rejected that contention on the basis that the IP rights of the claimant outweighed the relevant rights under Art 10 ECHR. When outlining the terms of the order, Justice Arnold engaged in a direct comparison between the Norwich Pharmacal doctrine and blocking injunctions under Article 8(3). However, the comparison was made principally for costs purposes as opposed to any substantive discussion about proportionality of relief.[74]

Again, when outlining the terms of a blocking injunction against ISPs restricting access to The Pirate Bay peer-to-peer file sharing platform[75], none of the ISPs in question raised an argument on the basis of data protection or privacy, and therefore Arnold J concluded that the terms agreed were proportionate between the Claimant's rights and the user's rights.[76] As Arnold J pointed out at first instance in *Cartier*, from *Newzbin 2* onwards none of the ISPs in question disputed the grant of the injunction, but rather they confined themselves to negotiating the terms of the order, resulting in many decisions being decided on the papers.[77]

The lack of opposition from ISPs does not preclude the court from accessing the proportionality of blocking injunctions, but illustrates that data protection has certainly not been used in this context as a tool to frustrate enforcement. In many of the aforementioned decisions, the terms of the orders were restricted to blocking and re-routing various IP addresses of the infringing sites, along with URL blocking to prevent user access to the domain and subdomain names.[78] Given that none of the terms imposed on the ISPs involved any disclosure of personal information, interference with data protection and privacy rights did not offer any ground for objection.

---

[69] It was however transposed into French law into Art. L. 716-6 of the IP Code, pursuant to which a court may, upon the request of a party (entitled to bring trademark infringement proceedings), order an intermediary to take any steps to put an end to the infringement. As for the French right to information of Art. L. 716-7-1 this type of order may only be obtained on an *inter partes* basis.

[70] *Cartier International AG and others v British Sky Broadcasting Ltd and others* [2014] EWHC 3354

[71] *Cartier International AG and another v British Sky Broadcasting Ltd and another* [2016] EWCA Civ 658

[72] [2011] EWHC 1981 (Ch)

[73] [2011] EWHC 2714 (Ch)

[74] *Twentieth Century Fox Film Corporation v British Telecommunications (Newzbin 2) (No.2)* [2011] EWHC 2714 [19] to [33]

[75] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268

[76] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No 2)* [2012] EWHC 1152

[77] [2014] EWHC 3354, [4]

[78] Under French law, it is also possible, in case of cybersquatting or typosquatting for instance, to request the AFNIC (the entity in charge of operating a number of French country code top-level domain names such as .fr, .re and .tf) to disclose the identity and address of the registrant of a domain name (by default anonymous). This is however not automatic: a trademark owner would have to show AFNIC a "legitimate reason" for it to lift the registrant's identity. If AFNIC refuses to disclose the registrant's identity, a mark owner would still have the possibility to petition, based not on IP-specific but on "traditional" rules of civil procedure, the pre-trial judge for an injunction (see for instance Versailles Tribunal of First Instance, 24 April 2007).

Unlike the position at national level, the CJEU in *Scarlet Extended SA v SABAM*[79] had the opportunity in the context of Article 8(3) of the Infosoc Directive to consider the interplay between IP enforcement and the right to the protection of personal data. The injunction sought in *Scarlet* involved the installation of a filtering system for all electronic communication made on the ISP's network regarding the right holders' copyright. The monitoring had no time limitation and was concerned with protection of current and future rights.[80]

The CJEU concluded that the obligation under the injunction sought would amount to an obligation to actively monitor all data relating to each of its customers in order to prevent any future infringement of intellectual property rights. Accordingly, the CJEU held that the injunction would interfere with the right to protection because the monitoring would involve a systematic analysis of users' IP addresses, which constitutes personal data because it allows individual users to be identified. The decision in *Scarlet* is an example of how data protection can be used to frustrate IP enforcement if the scope of the blocking injunction sought is so wide that the monitoring obligations would involve a disproportionate interference with personal data.

In a trade mark context, data protection was not considered a live issue by Arnold J in assessing the proportionality of the injunction granted against the ISPs in *Cartier*.[81] In his assessment of proportionality, Arnold J identified the property right of the claimants, the right of the ISPs to conduct their business freely, and the third party users' freedom to use the internet, as the rights engaged by the injunction. On appeal, the ISPs alleged that Arnold J failed to consider the impact of the monitoring requirements of the blocking measures on the ISPs' subscribers. It was argued that the blocking measure required the ISPs to use deep-packet-inspection technology or proxy servers, both of which involved real-time monitoring and invasive analysis of all subscribers' communications.

At first instance, Arnold J concluded that the measures did not constitute an overly intrusive interference, reasoning that the ISPs already had blocking measures in place in accordance with the Internet Watch Foundation, which could be used to block the IP addresses, domains and URLs of the infringing websites. On appeal, Kitchin LJ flatly rejected the argument that Justice Arnold failed to appreciate the impact of the blocking measures upon data protection and privacy rights of ISPs' subscribers, stating that the judge had given due consideration to the proposed blocking measures in the course of his judgement.[82] Unlike the blocking measures proposed in *Scarlet*, neither Arnold J nor Kitchin LJ felt that the technical means for blocking the infringing content amounted to a systematic analysis of all subscribers' data, and therefore would not impinge on their privacy or data protection rights.

Accordingly, in the context of blocking counterfeit websites, the privacy and data protection rights of individual users have not been preventing the grant of orders restricting the accessibility of such counterfeit websites. Implementing the technical means to block websites/IP addresses does not require an analysis of user data; it simply ensures the end goal website hosting the counterfeit material is blocked from access.

[79] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs* [2012] E.C.D.R. 4
[80] [2012] E.C.D.R. 4
[81] [2014] EWHC 3354 (Ch)[184]-[196]
[82] [2016] EWCA Civ 658 [182] to [183]