Neutral Citation Number: [2014] EWHC 3354 (Ch)

Case No: HC14C01382

IN THE HIGH COURT OF JUSTICE
CHANCERY DIVISION

Rolls Building
Fetter Lane, London, EC4A 1NL

Date: 17 October 2014

Before :

THE HON MR JUSTICE ARNOLD

- -

Between :

(1) CARTIER INTERNATIONAL AG **(2) MONTBLANC-SIMPLO GMBH** **(3) RICHEMONT INTERNATIONAL SA**	**Claimants**
- and -	
(1) BRITISH SKY BROADCASTING LIMITED **(2) BRITISH TELECOMMUNICATIONS PLC** **(3) EE LIMITED** **(4) TALKTALK TELECOM LIMITED** **(5) VIRGIN MEDIA LIMITED**	**Defendants**
- and -	
OPEN RIGHTS GROUP	**Intervener**

- -
- -

Adrian Speck QC and **Benet Brandreth** (instructed by **Wiggin LLP**) for the **Claimants**
Charlotte May QC and **Jaani Riordan** (instructed by **Reed Smith LLP**) for the **Defendants**
David Allen Green of **Preiskel & Co LLP** made written submissions on behalf of the **Intervener**

Hearing dates: 25-26 September 2014

- -

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

THE HON MR JUSTICE ARNOLD

MR JUSTICE ARNOLD :

Contents

Introduction

1. The Claimants (collectively, "Richemont") are the owners of a large number of United Kingdom Registered Trade Marks for CARTIER, MONTBLANC, IWC and other brands ("the Trade Marks"). The Defendants ("Sky", "BT", "EE", "TalkTalk" and "Virgin", collectively "the ISPs") are the five main retail internet service providers in the United Kingdom. Between them, they have a market share of some 95% of UK broadband users. By this application Richemont seek orders requiring the ISPs to block, or at least impede, access by their respective subscribers to six websites which advertise and sell counterfeit goods ("the Target Websites"). Richemont contend that the operators of the Target Websites thereby infringe the Trade Marks. For the avoidance of doubt, there is no suggestion that the ISPs have infringed the Trade Marks or are liable for infringements by the operators of the Target Websites.

2. The application raises five main questions. First, does this Court have jurisdiction to make an order of the kind sought? Secondly, if the Court has jurisdiction, what are the threshold conditions, if any, which must be satisfied if the Court is to make an order? Thirdly, are those conditions satisfied in the present case? Fourthly, if those conditions are satisfied, what are the principles to be applied in deciding whether or not to make such an order? Fifthly, applying those principles, should such orders be made in the present case?

3. Over the last three years, a series of orders have been made requiring the ISPs to block, or at least impede, access to websites pursuant to section 97A of the Copyright, Designs and Patents Act 1988 ("the 1988 Act"), which implements Article 8(3) of European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society ("the Information Society Directive"). I have considered the principles to be applied to applications of that kind in a series of judgments: *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch), [2012] Bus LR 1471 ("*20C Fox v BT*"); *Twentieth Century Fox Film Corp v British Telecommunications plc (No 2)* [2011] EWHC 2714 (Ch), [2012] Bus LR 1525 ("*20C Fox v BT (No 2)*"); *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch), [2012] 3 CMLR 14 ("*Dramatico v Sky*"); *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No 2)* [2012] EWHC 1152 (Ch), [2012] 3 CMLR 15 ("*Dramatico v Sky (No 2)*"); *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch), [2013] ECDR 8 ("*EMI v Sky*"); *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch), [2013] ECDR 14 ("*FAPL v Sky*"); and *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch), [2014] ECDR 7 ("*Paramount v Sky*"). Since the last of those judgments, Henderson J has considered the impact of the judgment of the Court of Justice of the European Union in Case C-466/12 *Svensson v Retriever Sverige AB* [EU:C:2014:76] in *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2014] EWHC 937 (Ch) ("*Paramount v Sky 2*").

4. It is convenient to note at this stage three points about the cases under section 97A. The first is that neither the ISPs nor the rightholders have appealed against any aspect of the orders made in those cases, including those aspects which deal with the costs of the applications and the costs of implementing the orders. The second is that, since

20C Fox v BT and *20C Fox v BT (No 2)*, the ISPs have not opposed the making of the orders sought by the rightholders, but have restricted themselves to negotiating the wording of the orders if the Court is minded to grant them. Thirdly, in consequence, most of the orders have been granted after consideration of the applications on paper.

5. The present application raises different considerations, for two main, linked reasons. The first is that the present case involves an attempt to combat trade mark infringement rather than copyright infringement. The second is that there is no statutory counterpart in the field of trade marks to section 97A of the 1988 Act. In addition, the arguments raised on the present application have differed to some extent from those raised in *20C Fox v BT*. For all these reasons, I have endeavoured to approach this application afresh. Inevitably, however, much of what was said in the judgments listed in paragraph 3 above is relevant. In addition, the experience that has been gained as a result of the orders granted in those cases is also relevant, as I shall explain.

6. I was informed by counsel that, so far as they and their professional and lay clients are aware, this is the first occasion on which an application for a website-blocking order against internet service providers in order to combat trade mark infringement has been made anywhere in the European Union, with the possible exception of the Danish case of *Home A/S v Telenor A/S* (Retten på Frederiksberg, 14 December 2012). It is a test case, which, if successful, is likely to be followed by other applications by Richemont and other trade mark owners, both here and in other countries.

7. The Open Rights Group ("the ORG") applied for permission to intervene in order to make some brief, moderate and helpful written submissions which focussed on the position of third parties who are potentially affected by the orders sought by Richemont. Sensibly, this application was not opposed by any of the parties and I therefore granted it. I am grateful to the ORG for its contribution.

Evidence

8. I have received a considerable volume of evidence on this application. I do not consider that it is necessary to summarise all the evidence in this judgment, although I have taken it all into account. There are two categories of evidence which merit specific comment.

9. First, an employee of each of the ISPs has made a witness statement describing that ISP's blocking technologies. Furthermore, each of the witnesses has given evidence about the historic costs which the ISP has incurred, as well as estimates of likely future costs if the orders sought are granted. As a result, I now have a much more complete and up-to-date picture than I did previously.

10. Secondly, both sides have served expert evidence. Richemont have served two expert reports from Helen Saunders. She is an independent contractor for (among others) Incopro Ltd, which specialises in the provision of technical services to assist in combating online intellectual property infringement. Ms Saunders has both an LLB and an LLM from Queen Mary University of London. She was previously employed by the Metropolitan Police Service, the former National Hi-Tech Crime Unit and Serious Organised Crime Agency, International Federation of the Phonographic Industry and British Phonographic Industry Ltd. In her first report, Ms Saunders

attempted to quantify the effect of the section 97A orders that have been granted. In her second report, Ms Saunders expanded and updated her analysis and responded to a number of points made by Professor Brown.

11. The ISPs served an expert report from Professor Ian Brown. Professor Brown has a BSc in Computer Science and Psychology from Newcastle University and a PhD in Computer Science from University College London. He is Professor of Information Security and Privacy at the University of Oxford, Senior Research Fellow at the Oxford Internet Institute and Associate Director of the University's Cyber Security Centre. His research is focussed on information security, privacy-enhancing technologies and internet regulation. In his report, Professor Brown provided a general introduction to website blocking technology, commented on the effectiveness of blocking orders, discussed evasion of website blocking and analysed the Target Websites.

Factual background

The problems of counterfeit goods and online trade mark infringement

12. A study published in 2008 by the Organisation for Economic Co-operation and Development ("OECD") entitled *The Economic Impact of Counterfeiting and Piracy* estimated that the value of counterfeited and pirated goods moving through international trade alone in 2005 amounted to up to US$200 billion. In 2011 Frontier Economics Ltd published a report entitled *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy* which estimated that the value of internationally traded counterfeit and pirated goods would increase to US$960 billion by 2015. In 2014 the European Commission published its *Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border* which recorded that in 2012 customs authorities at the external borders of the EU seized a total of over 39.9 million articles, representing a market value of almost €900 million. The corresponding figures for 2013 were 35.9 million articles and €768 million. The UK seized more articles than any other Member State.

13. The internet has become an increasingly important channel of trade in counterfeit goods. The OECD study noted that the online environment was attractive to counterfeiters for a number of reasons, including anonymity, flexibility, the size of the market, market reach and the ease of deceiving consumers. The European Commission report noted that the top six categories of goods seized (measured by number of cases) were the kind of goods often shipped by post or courier after an order via the internet.

14. The sale of counterfeit goods is damaging to trade mark owners like Richemont in at least four ways. First, they may lose sales. Where goods are advertised as replicas and sold at a fraction of the price charged for the genuine articles, then it is unlikely that consumers will be deceived and hence that the trade mark owner will have lost a sale at that point. But there may be occasions when a purchaser starts by intending to purchase a genuine article, but is tempted by an advertisement for a cheaper replica to buy that instead. In any event, such goods may subsequently be sold in a manner which deceives the purchaser into believing that the goods are genuine, in which case the trade mark owner may lose a sale then. Secondly, counterfeit goods are almost always of lower quality than the genuine articles. The circulation of substandard

counterfeit goods which are not easily distinguished from the genuine articles can easily damage the reputation of the latter, for example when the counterfeits are used as gifts. Thirdly, where the genuine articles were luxury goods with a cachet that depends in part upon their expense, and hence exclusivity, this is eroded by the availability of cheaper replicas. Fourthly, the availability of counterfeit goods may have the effect of damaging the confidence of some consumers in the legitimate market for such goods.

Richemont and the Trade Marks

15. Richemont are subsidiaries of Compagnie Financière Richemont SA. The Richemont group are producers and retailers of luxury goods. The Richemont group achieved total sales of €10,649 million in the year ending 31 March 2014. The Richemont group owns a number of well known brands, including Cartier, Montblanc and IWC. The Cartier brand dates back to 1847 when Louis-Francois Cartier established a jewellery business in Paris. Cartier opened its first boutique in London in 1902. Today, Cartier is well known for its jewellery and watches, and also sells leather goods, writing instruments and a range of other accessories. Montblanc was founded in 1906. It is well known for its writing instruments, and also sells watches, leather goods and a range of related accessories. IWC is a Swiss watch manufacturer which was founded in 1868. Cartier, Montblanc and IWC are all brands which have a considerable cachet: the goods bearing these brand names are expensive luxury items. Accordingly, exclusivity is an important aspect of the image of all three brands.

16. As indicated above, Richemont own a considerable number of Trade Marks. It is not necessary for the purposes of this judgment to set out all the Trade Marks upon which Richemont rely. By way of example, they include:

    i) UK Trade Mark No. 642,791 for the word CARTIER registered as of 10 December 1945 in respect of "jewellery, articles not included in other classes, made of precious metal or coated therewith precious stones clock, and watches [sic]" in Class 14.

    ii) UK Trade Mark No. 1,095,932 for Cartier in cursive script as shown below registered as of 22 May 1978 in respect of a wide range of goods including "precious metals and their alloys, jewellery, articles included in Class 14 made of precious metal or coated therewith, precious and semi-precious stones, clocks and watches" in Class 14.

    iii) UK Trade Mark No. 1,271,649 for the word MONTBLANC registered as of 18 July 1986 in respect of "writing and drawing instruments, stationery; inks and erasers, all included in Class 16; parts and fittings included in Class 16 for all the aforesaid good" in Class 16.

iv) UK Trade Mark No. 1,271,649 for the device shown below registered as of 29 June 1988 in respect of "Writing instruments, pouches for writing instruments, gift cases for writing instruments, inks and refills, stationery, desk sets; all included in Class 16" in Class 16.

v) International Trade Mark No. 729,301 for the letters IWC in a particular font protected in the UK with effect from 15 September 2000 in respect of "watches and parts thereof" in Class 14.

The Target Websites

17. Originally, the Target Websites in respect of which orders were sought by Richemont were seven websites located at the following URLs: www.cartierloveonline.com; www.hotcartierwatch.com; www.iwcwatchtop.com; www.replicawatchesiwc.com; www.1iwc.com; www.montblancpensonlineuk.com; and www.ukmontblancoutlet.co.uk. During the pendency of these proceedings, the website which was located at www.hotcartierwatch.com has gone offline, and so no order is now sought by Richemont in respect of that website. In addition, as I shall explain below, www.ukmontblancoutlet.co.uk has become www.montblancoutletonline.co.uk.

18. The remaining six Target Websites all advertise and sell counterfeit goods. Each Target Website sells replicas of a single brand, that is to say, either Cartier or Montblanc or IWC. In each case, the Target Website incorporates the brand name in its domain name. Some of the Target Websites make it very clear that the goods offered are replicas, whereas others make this much less clear. As discussed in more detail below, each of the Target Websites targets consumers in the UK (among other countries). Richemont have adduced evidence of a trap purchase from each Target Website by a purchaser resident in the UK. Furthermore, Richemont have adduced detailed and convincing evidence that all of the articles purchased in this way were both counterfeit and of significantly lower quality than the genuine articles.

19. It is not necessary for the purposes of this judgment to describe all of the Target Websites in detail, but I will briefly describe one by way of example. I will take www.cartierloveonline.com simply because it is the first. The home page is headed with the Cartier trade mark in cursive script. The top of the page also has a registration/signing in facility, a search function, links to "my account" and "shopping cart" and tabs to select USD, GBP or EUR. There is both a horizontal menu near the top of the page and a vertical menu extending down the left hand side of the page which list different categories of product such as "Cartier Bracelet", "Cartier Ring" and so on. Clicking on the entries in these menus leads to further pages of the website. The home page also features images of a series of products, described as "hot sales", at apparently discounted prices. For example, the first product shown is captioned "Cartier Love Bracelet mens White Gold with 4 Diamonds 20cm ~~£231.35~~ Now £59.48".

20. Scrolling down to the bottom of the homepage, one finds firstly six paragraphs of text about Cartier and then the following text:

> "**About cartierlove2u.com**
>
> Online Shop cartierlove2u.com is one professional replica cartier shop store. From the Cartier category on the left of site you can find each series of Cartier replica . you can find the different bracelet for men or ladies and Ordinary cartier or Cartier 1:1 Grade We do it carefully that you can shop here convenient and easily. And we have the abundant resources and multiple trade channels for each kind of replica Cartier love bracelet online. All Watches in cartierlove2u.com are in cheapest price but with the best service, and all of them are as accurate as those genuine one. If you have any problems when shopping on our site, just be free to contact our customer service staff at any time, we will be online for 24 hours in turn. You can consider the best sold watches in our site, which is most popular online. All the watches provides the detailed package, usually in two weeks, you can receive your ordered cartier by EMS freely."

21. Richemont's evidence is that on 1 February 2014 the website was offering 127 "Cartier" bracelets, 43 "Cartier Love" items, 35 "Cartier" necklaces, 16 "Cartier" earrings, 4 "Cartier" pendants and 7 types of "Cartier" box. By selecting a product, the user can obtain further information about that product. The information provided typically includes a photograph and a description of the product, an item ID number, the price and details of the product's availability and delivery and returns information. A number of the images include the Cartier mark and/or Cartier-branded products or packaging. Customer reviews may also be available.

22. On 30 December 2013 a test purchase was made from the website of a "Cartier 18K White Gold Love Bracelet with 4 Diamonds". Although the website purported to accept payment by Visa card, after the purchaser had placed his order he received an email advising him that the payment had failed and that he should make payment via www.aliexpress.com. Subsequently the purchaser received a package containing a counterfeit bracelet. The package identified the country of origin as China.

23. The website is targeted at (among others) UK consumers, as can be seen from the following: it is in English, sterling is among the currencies in which prices are displayed and orders from the UK are accepted and fulfilled.

24. As at February 2014, the domain name www.cartierloveonline.com was registered to a registrant with an address in Shanghai, China and the website was hosted on servers in San Jose, USA. Having previously been a mirror site for www.cartierlove2u.com, this URL now re-directs to www.cartierlove2u.net. As at 18 September 2014, the website shared an IP address with 11 other websites (as to which, see further below).

Blocking techniques in general

25. There are a number of methods of attempting to block access to websites that can be employed by providers such as the ISPs. Four such methods are as follows:

i) *DNS name blocking*. The Domain Name System (DNS) is the system that associates a domain name (such as www.cartierloveonline.com) with the Internet Protocol (IP) address (such as 23.238.175.169) that the ISPs use to route traffic to the web server that is hosting the website in question. The ISPs operate DNS servers that their customers' computers automatically call upon to look up IP addresses corresponding to DNS names. The customers' computers request these lookups so that they can address their communications to the website in question using its IP address, which is the necessary form of address for their communications to be delivered. DNS name blocking involves an ISP removing or modifying its records of the IP address(es) for a particular DNS name, so that when the ISP's DNS server is asked by a customer's computer for the IP address corresponding to the DNS name, the ISP's system either returns no IP address or points the customer to an IP address defined by the ISP that in actuality does not correspond to the DNS name.

ii) *IP address blocking using routers*. This is implemented in network devices which the ISPs operate known as border gateway (edge) routers that send customer communications to their destinations based on the destination IP addresses of the communications. An ISP can configure its routers to discard communications destined for the IP address of the website in question or route them to an IP address defined by the ISP that is different from the actual IP address of the website. This method thus blocks a customer's communications to a website even if the customer's computer uses the correct IP address for the website.

iii) *DPI-based URL blocking.* This method involves monitoring traffic by means of Deep Packet Inspection (DPI) and blocking requests for specific Uniform Resource Locators (URLs). A URL is a web address, which usually consists of the access protocol (e.g. http), the domain name (e.g. www.example.com) and the specific resource (i.e. the page e.g. main-page), separated by a colon and slashes. This method does not involve detailed, invasive analysis of the contents of the packets in the traffic (and for that reason it is sometimes referred to Shallow Packet Inspection rather than Deep Packet Inspection). It is typically implemented using proxy servers. It can also be used to implement IP address blocking as an alternative to the router method described above.

iv) *Two-stage systems.* Some ISPs operate two-stage systems. Typically this involves a first stage of IP-address re-routing and a second stage of DPI-based URL blocking. The first stage detects whether a customer's web request relates to an IP address on which some blocked content is hosted. If there is a match, the request is re-directed to the second stage; otherwise it is passed on normally. In the second stage traffic that relates to a blocked URL (or IP address) is stopped. The second stage is typically implemented using proxy servers.

Circumvention techniques

26. Each of the techniques described above can readily be circumvented by users who have a little technical knowledge and the desire to do so. DNS name blocking is the easiest to circumvent, but the other techniques can also be circumvented without difficulty. There are various methods that can be used, including proxy servers, virtual private networks and Tor. Prof Brown's evidence is that, since 2011, such circumvention methods have become more widely available and easier to use. Prof Brown also points out in paragraphs 144-146 of his report that there is one method of circumvention which is increasingly widely used, which does not even require users to use any special software or to make other changes to their device and which is particularly relevant in the context of the present application (as distinct from the section 97A context).

27. In addition to the methods available to users, there are circumvention methods which can be used by website operators, including changing IP addresses and URLs. These can be combated by updating the IP addresses or URLs that are blocked.

The Internet Watch Foundation's blocking regime

28. I described the Internet Watch Foundation ("IWF") and its blocking regime in *20C Fox v BT* at [65]-[69]. In summary, the IWF aims to minimise the availability of images of child sexual abuse on the internet. To this end, the IWF produces a list of URLs, updated twice daily, that contain images of child abuse. The URLs may be for whole domains, but more commonly they are for subdomains or specific pages. This list is supplied in encrypted form to the ISPs, who then implement automated blocking measures to prevent, or at least impede, access to these URLs by their subscribers. In addition to the blocking regime, the IWF operates a notice and takedown regime to remove such images from websites hosted in the UK.

29. As described below, each of the ISPs has invested in blocking technology to enable it to implement the IWF blocking regime. A point which is emphasised in the ISPs' evidence is that, because the IWF regime is automated, it requires very little human intervention by the ISPs and thus the operating costs are relatively low.

Sections 17 and 18 of the Digital Economy Act 2010

30. Sections 17 and 18 of the Digital Economy Act 2010 enabled the Secretary of State for Culture, Media and Sport to empower the courts to make orders requiring ISPs and other intermediaries to prohibit access to websites on the internet which were involved in infringing copyright. On 1 February 2011 the Secretary of State requested OFCOM to review these provisions. On 27 May 2011 OFCOM published a report entitled *"Site Blocking" to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*. In this report OFCOM concluded that, to quote from the executive summary:

> "**All [blocking techniques] can be circumvented to some degree by users and site owners who are willing to make the additional effort.**

> For all blocking methods circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users. Techniques are available for tackling circumvention, but these are of limited value against sophisticated tools, such as encrypted virtual private networks (VPN).
>
> **Nevertheless, sites blocking could contribute to an overall reduction in online copyright infringement – especially if it forms part of a broader package of measures to tackle infringement.**
>
> Just because it is technically possible for site operators and end users to circumvent blocking, it does not mean that in practice they will universally do so. The extent to which consumers and site operators will seek to circumvent blocking depends on a wide range of factors. These include the convenience and prevalence of circumvention techniques, the relative attractiveness of legal alternatives (and the opportunity costs of the illegal service foregone) and the ease and efficacy with which site operators can interact with the legal process should they dispute a block.
>
> Although imperfect and technically challenging, site blocking could nevertheless raise the costs and undermine the viability of at least some infringing sites, while also introducing barriers for users wishing to infringe. Site blocking is likely to deter casual and unintentional infringers and by requiring some degree of active intervention raise the threshold even for determined infringers.
>
> **The location of infringing sites can be changed relatively easily in response to site blocking measures, therefore site blocking can only make a contribution if the process is predictable, low cost and fast to implement.**
>
> …
>
> **We do not consider that sections 17 and 18 would be effective for generating lists of sites to be blocked.**"

31. The report went on to identify a number of features which a site blocking regime would need to have to increase the likelihood of success. Most of these features have been implemented in whole or in part in the section 97A orders.

32. An application for judicial review of section 17, and other provisions, of the 2010 Act was largely dismissed by Kenneth Parker J on 20 April 2011 (see *R (British Telecommunications Plc) v Secretary of State for Business, Innovation & Skills* [2011] EWHC 1021 (Admin), [2011] 3 CMLR 5). Nevertheless, on 3 August 2011 the Government announced that it did not intend to bring sections 17 and 18 of the 2010 Act into force. (An appeal by BT and TalkTalk to the Court of Appeal with respect to

the other provisions was also largely unsuccessful: see *Regina (British Telecommunications plc and another) v Secretary of State for Culture, Olympics, Media and Sport* [2012] EWCA Civ 232, [2012] BusLR 1766.) Clause 41 of the Deregulation Bill, which has been passed by the House of Commons and will reach Committee stage in the House of Lords on 21 October 2014, will repeal sections 17 and 18 of the 2010 Act.

Parental control services

33. Over the last three years, the ISPs have responded to Government and public pressure by making parental control services available to their subscribers. Recommendation 5 in *Letting Children be Children*, the report of an Independent Review of the Commercialisation and Sexualisation of Childhood by Reg Bailey which was presented to Parliament by the Secretary of State for Education in June 2011 (Cm 8078, "the Bailey Report"), was as follows:

> "**Making it easier for parents to block adult and age-restricted material from the internet:** To provide a consistent level of protection across all media, as a matter of urgency, the internet industry should ensure that customers must make an active choice over what sort of content they want to allow their children to access. To facilitate this, the internet industry must act decisively to develop and introduce effective parental controls, with Government regulation if voluntary action is not forthcoming within a reasonable timescale. … "

34. On 28 October 2011 Sky, BT, TalkTalk and Virgin agreed a Code of Practice on Parental Controls in which those ISPs recognised that "ISPs are well placed to deliver tangible progress to better protect children online, specifically through the advanced use of parental controls". Accordingly, they committed to offering new customers an enforced choice at the point of purchase, installation or activation of their service as to whether or not to use controls provided by their ISP to filter access to the internet free of charge by October 2012 at the latest.

35. In May 2013 the Department for Education published a Progress Report reviewing the progress that had been made in implementing the Bailey Report. In relation to recommendation 5, the Progress Report stated that there had been "good progress". After referring to the Sky, BT, TalkTalk and Virgin Code of Practice, the Progress Report went on:

> "These four ISPs, together with [EE], have gone further still, committing to provide whole-home filtering solutions to protect all devices in the home and will make setting up internet controls an unavoidable step for parents."

36. On 22 July 2013 the Prime Minister announced that Sky, BT, TalkTalk and Virgin had agreed to offer all new customers family-friendly network level filtering by the end of December 2013. The Department of Culture, Media and Sport subsequently asked OFCOM to review the measures which these ISPs had implemented to meet this commitment. On 22 July 2014 OFCOM published a *Report on Internet Safety Measures* describing and assessing these measures. The report noted that all four ISPs

had introduced appropriate measures, although Virgin had only done so in February 2014. I shall describe the measures used by the ISPs below. The report included the following assessments of these measures:

"**Circumventing filters**

5.9 There is a broad consensus that all filtering solutions face risks of circumvention, by a dedicated and technically competent user, supported by a range of advice available online. All four ISPs provide their subscribers with advice about the complementary actions they should take, as parents, to help secure their children's online safety.

5.10 Although the possibility of filter circumvention remains, each ISP has taken some steps to limit the extent of circumvention. For example, ISPs include lists of "proxy sites" whose primary purpose is to bypass filters or increase user anonymity as part of their standard blocking lists. In some cases, specific adaptations have been introduced to the filtering system to maintain blocks on sites which use encryption (such as Facebook and Twitter) but to which parents wish to restrict access. However, the use of wholly encrypted connections, as is the case when a VPN service is active, would bypass all selective filtering services.

Impact on internet access

5.11 Each ISP states that the filtering service has no impact on the general quality of the internet access service opted-in subscribers receive and that they undertake continuous monitoring to ensure this is the case. The primary concern about quality noted by the ISPs was over the possibility of incorrect categorisation of sites and services; and each ISP has processes in place, described in paragraphs 2.26 to 2.37 above, address reports of incorrect filter operation"

37. According to the report, the take up rate for these parental control services amongst new customers varies from 4.3% in the case of Virgin to 36% in the case of TalkTalk.

The ISPs' blocking systems

38. Each of the ISPs has invested in blocking systems to enable it to implement (a) the IWF blocking regime, (b) section 97A orders and (with the exception of EE) (c) parental controls. Each of the ISPs regards the technical and commercial details of these systems as sensitive confidential information. Nevertheless, for reasons that will become apparent, it is important for me to describe the systems at least in outline.

39. *Sky*. Since 2006 Sky has used a system known as Mohawk to implement the IWF blocking regime. Mohawk is a two-stage IP address re-routing and URL blocking system. Mohawk is able to block websites that are hosted on shared IP addresses

without blocking other websites hosted at the same address. Sky inherited Mohawk when it acquired Easynet.

40. In 2011 Sky developed a second system called Hawkeye. This is used for the sole purpose of implementing section 97A orders. Hawkeye is also a two-stage system, but it differs from Mohawk in operating on a pass-through rather than a proxy basis. Sky spent a six figure sum developing the system.

41. In November 2013 Sky launched its Sky Shield parental controls service. This is not provided by Hawkeye or Mohawk, but by a different system which implements DNS blocking. Sky Shield allows subscribers to choose a setting (PG, 13 or 18) which will block access to varying numbers of websites in 10 categories (including gaming, pornography and social networking). It also enables subscribers to block specific websites. There does not appear to be a limit to the number of sites which can be blocked.

42. *BT*. In 2004 BT launched a system known as Cleanfeed to implement the IWF blocking regime. Cleanfeed is a two-stage IP address re-routing and DPI-based URL blocking system (see *20C Fox v BT* at [73] and *20C Fox v BT (No 2)* at [6]). Cleanfeed is able to block websites that are hosted on shared IP addresses without blocking other websites hosted at the same address. BT spent a six figure sum purchasing the system and has spent the same amount subsequently on renewals and upgrades. In addition, five BT employees support this system, although as I understand it they also have other functions.

43. In 2012 BT acquired a second system called Nominum. Nominum is a DNS blocking system. Nominum is not able to block a website that shares a domain name with another website without blocking the latter. BT spent a seven figure sum purchasing this system. In addition, BT employs five people purely to support this system.

44. BT initially implemented section 97A orders using Cleanfeed. Currently it implements such orders using both Cleanfeed and Nominum.

45. Nominum is also used to provide BT's Parental Controls service, which was launched in December 2013. (BT also offers free downloadable Family Protection software developed in conjunction with McAfee which enables the user to protect a computer by, among other things, blocking inappropriate websites.) The Parental Controls service allows subscribers to block access to 17 broad categories of website (including pornography, gambling, social networking and games) and to block individual websites selected by the users. Users can set "light", "moderate" and "strict" filter options. There is no limit on the number of individual websites that the user can choose to block.

46. *EE*. Since at least 2014 EE has used a service called Procera which is supplied by BT (this service is distinct from Cleanfeed and Nominum). This system is described by witnesses from both BT and EE, although their descriptions are not entirely consistent with each other. Curiously, it appears from both witnesses' accounts that the system is capable of DPI-based URL filtering, but in the context of section 97A orders has only been used to implement IP address blocking. (This may be because the Procera system has replaced an earlier system called Arbor which was only capable of IP address blocking.) According to EE's witness, the Procera system also has other

functions, but a different system is used to implement the IWF blocking regime. The latter system is not described in EE's evidence. According to BT's witness, EE paid BT a seven figure sum to implement the Procera system in 2010 (*sic*) and pays BT a six figure monthly fee to operate it.

47. Unlike the other four ISPs, EE does not offer a network level parental controls service. Instead, it offers customers the option to buy parental control software developed by a third party which can be downloaded onto the user's computer.

48. *TalkTalk*. Since 2006 TalkTalk has used a system called Detica to implement the IWF blocking regime. It is not used for any other purpose. TalkTalk does not have a record of how much it spent on this system originally, but earlier this year it spent a six figure sum on upgrading it. In addition a four figure sum is spent on monthly running costs.

49. In 2009 TalkTalk acquired a second system supplied by Huawei, which was initially used to provide TalkTalk's HomeSafe parental controls service. HomeSafe has three aspects, one of which is Kid Safe, which enables subscribers to block nine categories of website (including pornography, gambling, games and social networking) and to block up to nine specific websites. The Huawei system is now also used to implement section 97A orders. The Huawei system implements DPI-based URL filtering. Total capital expenditure on this system since 2010 has been an eight figure sum. In addition, a six figure sum is spent on annual maintenance and running costs.

50. *Virgin*. From 2006 to 2012 Virgin has used a system called Web Blocker to implement the IWF blocking regime. In mid 2011 Virgin acquired a replacement system called Web Blocker 2. This system is a two-stage IP address re-routing and DPI-based URL blocking system. The purchase price of this system was a six figure sum. It was subsequently modified to enable implementation of section 97A orders. Ongoing support for the system is provided by a third party which costs a five figure sum annually.

51. In February 2014 Virgin launched its Web Safe parental controls service, one of the functions of which is Child Safe. Child Safe enables subscribers to block eight categories of websites (including pornography). It appears that Web Safe is provided by a different system to Web Blocker 2.

Section 97A orders obtained to date

52. To date, section 97A orders have been obtained by three groups of rightholders: (a) film studios, (b) record companies and (c) the FA Premier League.

53. The following orders have been granted pursuant to applications by film studios:

    i) an order dated 26 October 2011 in respect of Newzbin2 (see *20C Fox v BT* and *20C Fox v BT (No 2)*);

    ii) an order dated 24 April 2013 in respect of Movie2K and DL4all (plus an order dated 17 July 2013 when Movie2K became Movie 4K);

    iii) an order dated 1 July 2013 in respect of EZTV;

iv) three orders dated 25 October 2013 in respect of YIFY-Torrents and four other websites;

v) an order dated 13 November 2013 in respect of SolarMovie and Tube+ (see *Paramount v Sky*); and

vi) an order dated 18 February 2014 in respect of Viooz and three other websites (see *Paramount v Sky 2*).

54. The solicitor who has had the conduct of the applications listed above, Simon Baggs of Wiggin LLP, has given evidence as to the costs of an unopposed application for a section 97A order (which, in accordance with my decision in *20C Fox v BT (No 2)*, are borne by the rightholders). The detailed figures are confidential, but it works out at around £14,000 per website. This does not include the subsequent monitoring costs (as to which, see below).

55. The following orders have been granted pursuant to applications by record companies:

i) an order dated 13 June 2012 in respect of The Pirate Bay ("TPB") (see *Dramatico v Sky* and *Dramatico v Sky (No 2)*);

ii) an order dated 28 February 2013 in respect of Fenopy, H33T and Kat (see *EMI v Sky*); and

iii) an Order dated 8 October 2013 in respect of 1337X and 20 other websites.

56. Only one order has so far been obtained by the FA Premier League, namely an order dated 16 July 2013 in respect of FirstRow (see *FAPL v Sky*).

57. There is no evidence before me as to the costs incurred by these rightholders in making such applications, but it is safe to assume that they are of a similar magnitude to the costs incurred by the film studios.

Implementation of the section 97A orders by the rightholders

58. An important feature of all the orders made pursuant to section 97A has been that, as discussed in *20C Fox v BT (No 2)* at [10]-[12], they include provision for the rightholders to notify additional IP addresses and/or URLs to the ISPs in respect of the websites which have been ordered to be blocked. In this way the rightholders are able to respond to circumvention measures adopted by the website operators which involve changing IP addresses or URLs. As subsequent experience has confirmed, this is an important feature of the orders from a practical perspective.

59. As I stated in *20C Fox v BT (No 2)*, it is the rightholders' responsibility accurately to identify IP addresses and URLs which are to be notified to ISPs in this way. In order to discharge this responsibility, the film studios have engaged Incopro to monitor the server locations and domain names used by the targeted websites. Incopro maintains a regularly updated database of almost 10,000 websites which provide access to copyright-protected content. This database is used to identify IP addresses and domain names for targeted websites when the application is filed. Incopro also operates a system called BlockWatch, which continuously monitors the IP addresses and

domains for the targeted websites on an hourly basis by an automated process. This system is used to provide notifications to the ISPs after an order has been made. These notifications include notifications that an IP address previously dedicated to a target website has become shared with another, legitimate website and so should no longer be blocked.

60. Incopro charges a fee to enter a site into the BlockWatch system. It also charges an ongoing monthly fee. In addition, the rightholders incur legal costs in collating, checking and sending notifications to the ISPs. Mr Baggs' evidence is that, together, these costs work out at around £3,600 per website per year.

Implementation of the section 97A orders by the ISPs

61. *Sky*. Sky's evidence is that the cost of implementing a new order is a sum in the mid three figures while the cost of an update is around half that. In addition, Sky incurs monitoring costs in a low four figure sum per month. Sky estimates that the cost of implementing the order sought in this case would be a low four figure sum given that it is a new type of order.

62. *BT*. BT's evidence is that, at present, approximately 60 days of employee time per year are spent implementing section 97A orders using Cleanfeed and about 12 additional days of employee time per year are spent implementing section 97A orders using Nominum. Each new order takes about 8 hours of BT's in-house lawyers' time, 7 hours of the Cleanfeed team's time and 6 hours of the Nominum team's time to implement. Each update takes about 1 hour of BT's in-house lawyers' time, 7 hours of the Cleanfeed team's time and 6 hours of the Nominum team's time to implement. It is not clear from this evidence whether the costs incurred by BT are in excess of the estimate BT made at the time of the *20C Fox v BT* case of £5,000 for initial implementation and £100 for each subsequent notification (see *20C Fox v BT (No 2)* at [32]).

63. *EE*. Each new order takes about 30 minutes of EE staff time and about 3 hours of BT staff time to implement. As I understand it, updates take the same time. EE's evidence is that it pays BT a fee approaching four figures for each update. I assume that the fee for implementing the original order is about the same. In addition, about 36 hours are spent on yearly maintenance and management.

64. *TalkTalk*. TalkTalk's evidence is that implementation of a new order takes about two hours of legal personnel's time and about 2½ hours of an engineer's time. I assume that a similar amount of time is taken for updates. TalkTalk estimates that a total of approximately 60 days of a senior engineer's time is required each year to deal with the implementation of new orders and updates, costing a low six figure sum a year.

65. *Virgin*. Virgin's evidence is that three of its internet security staff are involved part-time in website blocking at an estimated cost of a low five figure sum per year. Virgin's evidence also includes a higher figure for implementation and updating of section 97A orders over the last year, but this figure includes substantial time spent by other personnel, and in particular time spent on responding to comments on social media. As I understand to be common practice among the ISPs, Virgin directs subscribers who attempt to access a blocked website to a page which informs them both that the site has been blocked and why, as shown below.

Problems encountered as a result of section 97A orders

66. On the whole, implementation of the section 97A orders appears to have proceeded smoothly. It would not be accurate to say that it has been entirely trouble free, however. Two problems have been encountered.

67. The first problem is that there have been a small number of incidents involving overblocking. In particular, on 9 August 2013 BT and Virgin blocked access to an IP address following a notification by the FA Premier League under the order in respect of the FirstRow website. The IP address in question hosted a number of websites that were not the subject of the order, including the *Radio Times* website. Access to those websites was blocked until 13 August 2013 when the situation was corrected. Although there is no evidence from the FA Premier League, it appears that there was an error in the notification. In December 2013 Sky blocked access to the media-sharing platform Imgur when implementing the order in respect of the YIFY-Torrents website. Mr Baggs' evidence is that this was due to the way in which Hawkeye operated in the rather unusual circumstances which pertained at the time rather than due to any error on the part of the rightholders. Even so, it is regrettable.

68. The second problem is that there have been a small number of incidents involving attacks of one kind or another. EE, TalkTalk and Virgin were subjected to "distributed denial of service" attacks on their websites for a short period following implementation of the order to block TPB. It is reasonable to suppose that this was attributable to the particular profile of TPB. In addition, both Sky and Virgin were the victims of "malicious DNS poisoning" when implementing the order to block EZTV, causing their subscribers to lose access briefly to certain prominent websites.

Applications for further section 97A orders

69. There are a number of pending applications for further section 97A orders. I have received the following unopposed applications for consideration on paper:

    i) An application by Paramount Home Entertainment Ltd and other film studios by application notice dated 29 July 2014 for orders in respect of seven websites which are said to be substantially focussed on infringement of copyright in films and television programmes.

    ii) An application by 1967 Ltd and other record companies by application notice dated 31 July 2014 for orders in respect of 21 websites which are said to be involved in peer-to-peer file sharing using BitTorrent.

    iii) An application by Twentieth Century Fox Film Corp and other film studios by application notice dated 29 August 2014 for orders in respect of eight websites which are said to be substantially focussed on infringement of copyright in films and television programmes.

70. Knowing that I would have the benefit of receiving adversarial argument and evidence in the present case, I have deferred decisions on those applications until after giving this judgment. The parties in the present case addressed me on the assumption that those applications were likely to be granted, and I shall consider this application on the same basis.

71. I was informed by counsel for the ISPs that a fourth application was either pending or would be made shortly. I have not yet received this application, but I shall proceed on the assumption that it will be made shortly. Again, I shall proceed on the basis that it is likely to be granted.

The orders sought

72. Richemont's application seeks orders against each of the ISPs in essentially the same form as the orders which have been granted by the Court in the most recent section 97A cases. The precise wording of these orders varies from ISP to ISP to take account of the different technologies they employ, but the general form of the orders is substantially as follows:

> "1. In respect of its residential fixed line broadband customers to whose service the system known as … is applied, the … Defendant shall within 15 working days in relation to the initial notification (and thereafter, within 10 working days of receiving any subsequent notification) adopt the following technical means to block or attempt to block access to the Target Websites, their domains and sub-domains and any other IP address or URL notified to the …. Defendant whose sole or predominant purpose is to enable or facilitate access to a Target Website. The technology to be adopted is:

(i) IP blocking in respect of each and every IP address from which each of the Target Websites operate and which is:

(a) notified in writing to the … Defendant by the Applicants or their agents; and

(b) in respect of which the Claimants or their agents notify the … Defendant that the server with the notified IP address does not also host a site that is not part of a Target Website.

(ii) IP address re-routing in respect of all IP addresses that provide access to each and every URL available from each of the Target Websites and their domains and sub-domains and which URL is notified in writing to the … Defendant by the Claimants or their agents; and

(iii) URL blocking in respect of each and every URL available from each of the Target Websites and their domains and sub-domains and which is notified in writing to the … Defendant by the Claimants or their agents.

2. For the avoidance of any doubt paragraphs 1(i), 1(ii) and 1(iii) are complied with if the … Defendant uses the system known as … to implement the steps required by those paragraphs.

3. The Claimants or their agents will notify the … Defendant should any IP address and/or URL which has already been notified to the … Defendant under the terms of this Order cease to enable or facilitate access to a Target Website (in which case the … Defendant shall no longer be obliged to block that IP address and/or URL). For the avoidance of doubt, the …. Defendant is wholly reliant on the Claimants accurately identifying the IP addresses and/or URLs from which the Target Websites operate and which should be blocked under the terms of this Order.

4. The … Defendant shall not be in breach of paragraphs 1(i), 1(ii) and/or 1(iii) if it temporarily suspends … or the addition of IP addresses or URLs thereto with the consent of the Claimants or their agents.

5. The proceedings shall be stayed, save for the purposes of any application to give effect to the terms of this order and save that the parties have permission to apply on notice in the event of any material change of circumstances including, for the avoidance of doubt but without limiting the generality of the foregoing, in respect of the costs, consequences for the parties

and effectiveness of the aforesaid technical means from time to time.

6. The operators of the Target Websites (as defined in the Schedule to this Order) and the operators of any other website who claim to be affected by this Order, are to have permission to apply on notice to vary or discharge this Order insofar as it affects such an applicant, any such application to be on notice to all the parties and to be supported by materials setting out and justifying the grounds for the application. Any such application shall clearly indicate the status of the applicant and indicate clearly (supported by evidence) that it is the operator of any website which is the subject of such application.

7. There be no order for costs."

The legal context

73. The principal legislative provisions which are relevant to this application are as follows.

Senior Courts Act 1981

74. Section 37(1) of the Senior Courts Act 1981 ("the 1981 Act", previously known as the Supreme Court Act 1981) provides as follows:

> "The High Court may by order (whether interlocutory or final) grant an injunction … in all cases in which it appears to be just and convenient to do so."

Trade Marks Directive and CTM Regulation

75. Article 5 of European Parliament and Council Directive 2008/95/EC of 22 October 2008 to approximate the laws of the Member States relating to trade marks (codified version) ("the Trade Marks Directive") provides, so far as relevant, as follows:

"*Article 5*

Rights conferred by a trade mark

1. The registered trade mark shall confer on the proprietor exclusive rights therein. The proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade:

   (a) any sign which is identical with the trade mark in relation to goods or services which are identical with those for which the trade mark is registered;

   …

3. The following, *inter alia*, may be prohibited under paragraphs 1 and 2:

(a) affixing the sign to the goods or to the packaging thereof;

(b) offering the goods, or putting them on the market or stocking them for these purposes under that sign, or offering or supplying services thereunder;

(c) importing or exporting the goods under the sign;

(d) using the sign on business papers and in advertising.

…"

Domestic implementation of the Trade Marks Directive

76. Article 5(1)(a) and (3) of the Directive were implemented in the United Kingdom by section 10(1) and (4) of the Trade Marks Act 1994 ("the 1994 Act"). The 1994 Act also contains the following provisions:

"**Registered trade marks**

2.(1) A registered trade mark is a property right obtained by the registration of the trade mark under this Act and the proprietor of a registered trade mark has the rights and remedies provided by this Act.

…

Rights conferred by registered trade mark

9.(1) The proprietor of a registered trade mark has exclusive rights in the trade mark which are infringed by use of the trade mark in the United Kingdom without his consent. The acts amounting to infringement, if done without the consent of the proprietor, are specified in section 10.

…

Action for infringement

14.(1) An infringement of a registered trade mark is actionable by the proprietor of the trade mark.

(2) In an action for infringement all such relief by way of damages, injunctions, accounts or otherwise is available to him as is available in respect of the infringement of any other property right.

Order for delivery up of infringing goods, material or articles

16.(1) The proprietor of a registered trade mark may apply to the court for an order for the delivery up to him, or such other

> person as the court may direct, of any infringing goods, material or articles which a person has in his possession, custody or control in the course of a business.
>
> …
>
> (4) Nothing in this section affects any other power of the court."

E-Commerce Directive

77. I set out recitals (7)-(8), (17), (20), (40), (42), (45)-(48) and (50) of European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("the E-Commerce Directive") in *20C Fox v BT* at [79]. For present purposes, the most relevant recitals are the following:

> "(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.
>
> (46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.
>
> (47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.
>
> (48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities."

78. I set out Articles 2(a),(b) and (d), 12, 13, 14, 15, 18(1) and 20 of the E-Commerce Directive in *20C Fox v BT* at [80] and [82]. For present purposes, the key provisions are as follows:

> "*Article 12*

'Mere conduit'

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

   (a) does not initiate the transmission;

   (b) does not select the receiver of the transmission; and

   (c) does not select or modify the information contained in the transmission.

…

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13

'Caching'

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

   (a) the provider does not modify the information;

   (b) the provider complies with conditions on access to the information;

   (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

   (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

   (e) the provider acts expeditiously to remove or disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to

it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14

Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

   (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

…

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information

Article 15

No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

Domestic implementation of the E-Commerce Directive

79. The E-Commerce Directive was transposed into domestic law by the Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013 ("the 2002 Regulations"). In particular, Articles 12-14 of the E-Commerce Directive are implemented by regulations 17-20 of the 2002 Regulations. There is little difference between the wording of the respective provisions, however, and it was not suggested by either side that they bore different meanings. Regulation 22 of the 2002 Regulations provides:

> "**Notice for the purposes of actual knowledge**
>
> In determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i), a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to—
>
> (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and
>
> (b) the extent to which any notice includes—
>
> (i) the full name and address of the sender of the notice;
>
> (ii) details of the location of the information in question; and
>
> (iii) details of the unlawful nature of the activity or information in question."

Information Society Directive

80. I set out recitals (4), (9)-(13), (16), (22) and (58)-(60) and Article 8 of the Information Society Directive in *20C Fox v BT* at [84]-[85]. For present purposes, it suffices to quote recital (59) and Article 8(3), which are in the following terms:

> "(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States."

> "8.(3) Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."

Domestic implementation of the Information Society Directive

81. The Information Society Directive was transposed into domestic law by the Copyright and Related Rights Regulations 2003, SI 2003/2498 ("the 2003 Regulations"). In particular, Article 8(3) was implemented by Regulation 27, which inserted sections 97A and 191JA into Parts I and II respectively of the CDPA 1988. Section 97A provides as follows:

> "**97A Injunctions against service providers**
>
> (1) The High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright.
>
> (2) In determining whether a service provider has actual knowledge for the purpose of this section, a Court shall take into account all matters which appear to it in the particular circumstances to be relevant and, amongst other things, shall have regard to –
>
> (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); and
>
> (b) the extent to which any notice includes –
>
> (i) the full name and address of the sender of the notice;
>
> (ii) details of the infringement in question.
>
> (3) In this section 'service provider' has the meaning given to it by regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002."

The Enforcement Directive

82. Recitals (17), (23) and (32) of European Parliament and Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights ("the Enforcement Directive") read as follows:

> "(17) The measures, procedures and remedies provided for in this Directive should be determined in each case in such a manner as to take due account of the specific characteristics of that

case, including the specific features of each intellectual property right and, where appropriate, the intentional or unintentional character of the infringement.

…

(23) Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right. The conditions and procedures relating to such injunctions should be left to the national law of the Member States. As far as infringements of copyright and related rights are concerned, a comprehensive level of harmonisation is already provided for in Directive 2001/29/EC. Article 8(3) of Directive 2001/29/EC should therefore not be affected by this Directive.

…

(32) This Directive respect the fundamental rights and observed the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Directive seeks to ensure full respect for intellectual property rights, in accordance with Article 17(2) of that Charter."

83. Articles 3, 9(1)(a) and 11 provide as follows:

"*Article 3*

General obligation

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.

Article 9

Provisional and precautionary measures

1. Member States shall ensure that the judicial authorities may, at the request of the applicant:

(a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the rightholder; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right; injunctions against intermediaries whose services are used by a third party to infringe a copyright or a related right are covered by Directive 2001/29/EC;

…

Article 11

Injunctions

Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC."

Domestic implementation of the Enforcement Directive

84. The Enforcement Directive was transposed into domestic law primarily by the Intellectual Property (Enforcement, etc.) Regulations 2006, SI 2006/1028. As discussed below, the UK did not take any specific steps to implement the third sentence of Article 11.

The Charter of Fundamental Rights of the European Union

85. The Charter of Fundamental Rights of the European Union ("the Charter") was originally proclaimed by the European Parliament, Council and Commission at Nice

in December 2000. As amended in December 2007, it became legally binding with the coming into force of the Lisbon Treaty in December 2009.

86. The Charter includes the following provisions:

"*Article 11*

Freedom of expression and information

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

…

Article 16

Freedom to conduct a business

The freedom to conduct a business in accordance with Union law and national laws and practices is recognised Article 17

Article 17

Right to property

….

2. Intellectual property shall be protected.

…

Article 51

Field of application

1. The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

2. The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties.

Article 52

Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

4. In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions.

5. The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality.

6. Full account shall be taken of national laws and practices as specified in this Charter.

7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States."

Relevant principles of interpretation

87. As discussed below, the application gives rise to a number of issues of interpretation of the legislation set out above. The following principles of interpretation are particularly relevant to these issues.

EU directives do not have horizontal effect

88. Directives are addressed to the Member States. It is a settled principle of EU law that a directive does not confer upon private litigants any rights capable of direct

enforcement against other private litigants. This is so regardless of how clearly, precisely and unconditionally it is phrased: Case C-12/08 *Mono Car Styling SA v Odemis* [2009] ECR I-6653 at [59].

Interpretation of domestic legislation in the context of EU directives

89. It is well established that domestic legislation, and in particular legislation specifically enacted or amended to implement an EU directive, must be construed so far as is possible in conformity with, and to achieve the result intended by, the directive: Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentación SA* [1990] ECR I-4135 at [8] and Cases C-397/01 to C-403/01 *Pfeiffer v Deutsches Rotes Kreuz, Kreisverband Waldshut eV* [2004] ECR I-8835 at [113]-[117]. This is a strong duty of interpretation. For a distillation of the relevant jurisprudence with regard to this duty, see *Vodafone 2 v Revenue and Customers Commissioners (No 2)* [2009] EWCA Civ 446, [2009] STC 1480 at [37]-[38] (Sir Andrew Morritt C).

Interpretation of EU directives

90. An EU directive falls to be interpreted according to principles of interpretation of EU legislation developed by the Court of Justice of the European Union. The basic rule of interpretation, which has been frequently reiterated by the CJEU, is that stated in Case C-306/05 *Sociedad General de Autores y Editores de España v Rafael Hoteles SA* [2006] ECR I-11519 at [34]:

> "According to settled case-law, in interpreting a provision of Community law it is necessary to consider not only its wording, but also the context in which it occurs and the objectives pursued by the rules of which it is part (see, in particular, Case C-156/98 *Germany v Commission* [2000] ECR I-6857, paragraph 50, and Case C-53/05 *Commission v Portugal* [2006] ECR I-6215, paragraph 20)".

91. As is well known, in applying this rule, the CJEU routinely refers to the recitals of the measure as well as its operative provisions, and frequently refers to pre-legislative materials such as the Explanatory Memoranda which accompany the Commission's legislative proposals.

Jurisdiction

The issue

92. As noted above, whereas the UK implemented Article 8(3) of the Information Society Directive by amending the 1988 Act to insert section 97A, the UK did not pass any legislation to implement the third sentence of Article 11 of the Enforcement Directive. This is despite the fact that the effect of the third sentence of Article 11 of the Enforcement Directive is to extend the requirement imposed on Member States by Article 8(3) of the Information Society Directive with regard to copyright and related rights to all forms of intellectual property. The ISPs contend that, as a consequence, this Court has no jurisdiction to make orders of the kind sought by Richemont. Richemont contend that the Court has jurisdiction to make such orders pursuant to section 37(1) of the 1981 Act (or, more accurately, the power which section 37(1)

recognises and confirms). Richemont advance this contention on two alternative bases. The first is that the Court has the necessary jurisdiction upon a purely domestic interpretation of section 37(1). The second is that, even if that is not the result of a purely domestic interpretation of section 37(1), section 37(1) can and should be construed consistently with the third sentence of Article 11 in accordance with the *Marleasing* principle.

93. I should make it clear before proceeding further that I am only concerned with the jurisdiction of this Court, that is to say, the High Court of England and Wales. I am not concerned with the jurisdiction of the High Court of Northern Ireland or that of the Court of Session in Scotland.

Domestic interpretation of section 37(1)

94. Prior to 1854 the only court which had power to grant injunctions was the Court of Chancery, which claimed an inherent jurisdiction to do so. The courts of common law had no such power. Section 79 of the Common Law Procedure Act 1854 conferred a statutory jurisdiction upon the common law courts. Section 16 of the Supreme Court of Judicature Act 1873 ("the Judicature Act") provided that the new High Court of Justice created by the Judicature Act should have the jurisdiction previously vested in, or capable of being exercised by, the Court of Chancery, the Court of Queen's Bench and various other superior courts. Section 25(8) of the Judicature Act provided that "an injunction may be granted … by an interlocutory order in all cases in which it shall appear to the court to be just or convenient that such order shall be made". Section 25(8) was replaced by section 45(1) of the Supreme Court of Judicature (Consolidation) Act 1925, which was in turn replaced by section 37(1) of the 1981 Act. The only difference between section 37(1) and its predecessors is that section 37(1) expressly recognises the Court's jurisdiction to grant a final, as opposed to an interlocutory, injunction.

95. The effect of section 25(8) of the Judicature Act, or now section 37(1) of the 1981 Act, was simply to make it clear that the High Court could grant an injunction in all kinds of case. It follows that, as Brett LJ put it in *North London Railway Co v Great Northern Railway Co* (1883) 11 QBD 30, 36–37, "if no court had the power of issuing an injunction before the Judicature Act, no part of the High Court has power to issue such an injunction now". It also follows that, as James LJ put it in *Day v Brownrigg* (1878) 10 ChD 294 at 307, "the power given to the Court by sect 25, sub-sect 8, of the Judicature Act, 1873, to grant an injunction in all cases in which it shall appear to the Court to be 'just or convenient' to do so, does not in the least alter the principles on which the Court should act." It does not follow, however, that either the Court's jurisdiction or the principles it applies as a matter of practice when deciding whether or not to grant an injunction are fixed by the statute. Still less does it follow that those principles are immutable.

96. The extent of the Court's power to grant an injunction has been considered by the House of Lords, the Privy Council and the Supreme Court in at least 12 cases in the last 40 years: *Gouriet v Union of Post Office Workers* [1978] AC 335, *The Siskina* [1979] AC 210, *Castanho v Brown & Root (UK) Ltd* [1981] AC 557, *British Airways Board v Laker Airways Ltd* [1985] AC 58, *South Carolina Insurance Co Ltd v Assurantie Maatschappij De Zeven Provincien NV* [1987] AC 24, *Pickering v Liverpool Daily Post* [1991] 2 AC 370, *Kirklees MBC v Wickes Building Supplies Ltd* [1993]

AC 227, *Channel Tunnel Group Ltd v Balfour Beatty Construction Ltd* [1993] AC 334, *Mercedes-Benz AG v Leiduck* [1996] AC 284, *Fourie v Le Roux* [2007] UKHL 1, [2007] 1 WLR 320, *Tasarruf Mevduati Sigorta Fonu v Merrill Lynch Bank & Trust Company* [2011] UKPC 17, [2012] 1 WLR 1721 and *Ust-Kamenogorsk Hydropower Plant JSC v AES Ust-Kamenogorsk Hydropower Plant LLP* [2013] UKSC 35, [2013] 1 WLR 1889.

97. Those authorities reveal a surprising divergence of views at the highest level. Analysis of the law is not helped by two factors. First, in many of these cases the effect of section 37(1) was only indirectly in issue. For example, in some of the cases the immediate issue was one of service out of the jurisdiction. Secondly, some of the dicta in these cases contain what at first blush appear to be comprehensive statements of the law which on closer reading are revealed not to be exhaustive.

98. In my judgment, the most authoritative statement of the law as it currently stands is to be found in the speech of Lord Scott of Foscote, with whom all the other members of the House of Lords agreed on this issue, in *Fourie v Le Roux*. Lord Scott's analysis can be summarised in three propositions. The first is that it is necessary to distinguish between the jurisdiction of the court - that is to say, its power to grant an injunction - and the practice of the court not to do so except in a certain way and under certain circumstances.

99. The second is his statement at [25]:

> "The power of a judge sitting in the High Court to grant an injunction against a party to proceedings properly served is confirmed by, but does not derive from, section 37 of the Supreme Court Act 1981 and its statutory predecessors. It derives from the pre-Supreme Court of Judicature Act 1873 (36 & 37 Vict c 66) powers of the Chancery courts, and other courts, to grant injunctions: see section 16 of the 1873 Act and section 19(2)(b) of the 1981 Act."

100. The third is the conclusion he drew at [30] from a review of many of the earlier authorities:

> "My Lords, these authorities show, in my opinion, that, provided the court has in personam jurisdiction over the person against whom an injunction, whether interlocutory or final, is sought, the court has jurisdiction, in the strict sense, to grant it. The practice regarding the grant of injunctions, as established by judicial precedent and rules of court, has not stood still since *The Siskina* [1979] AC 210 was decided and is unrecognisable from the practice to which Cotton LJ was referring in *North London Railway Co v Great Northern Railway Co* (1883) 11 QBD 30, 39–40 …"

101. In my view this statement of the law confirms the correctness of the analysis in Spry, *Equitable Remedies* (5th ed, 1997) at 323 which was cited with approval by Lord Woolf MR in *Broadmoor Special Hospital Authority v Robinson* [2000] QB 775 at [20]:

> "The powers of courts with equitable jurisdiction to grant injunctions are, subject to any relevant statutory restrictions, unlimited. Injunctions are granted only when to do so accords with equitable principles, but this restriction involves, not a defect of powers, but an adoption of doctrines and practices that change in their application from time to time. Unfortunately, there have sometimes been made observations by judges that tend to confuse questions of jurisdiction or of powers with questions of discretions or of practice. The preferable analysis involves a recognition of the great width of equitable powers, an historical appraisal of the categories of injunctions that have been established and an acceptance that pursuant to general equitable principles injunctions may issue in new categories when this course appears appropriate."

102. The same passage appears in the current (9th, 2014) edition of Dr Spry's book at 333. He deals with the same point more fully at pages 342-343 as follows (footnotes omitted):

> "Where, in England and in other jurisdictions, the superior courts now exercise the powers of the former Court of Chancery, whether or not they are also able to grant legal injunctions or are affected by special Judicature Act provisions, their powers of granting injunctions are unlimited, provided that they have jurisdiction over the defendant in the circumstances in question. These powers are however exercised in accordance with the principles set out here under.
>
> First, an injunction may issue in the protection of any legal right whatever, save for an applicable statutory provision provides to the contrary. For these purposes the relevant legal right must ordinarily be a present right of the plaintiff, as opposed to a right that he merely expects or hopes to acquire in the future.
>
> Secondly, an injunction may issue in the enforcement of any equitable right. Here on a strict analysis the right to the injunction itself represents pro tanto the equitable right in question. Hence in ascertaining whether an injunction may be obtained on this basis it is necessary to determine whether injunctions of the relevant kind were formally granted in the exclusive or concurrent jurisdiction of courts of equity, and if not, whether the principles underlying those jurisdictions should nonetheless now be treated as rendering the grant of the injunction appropriate.
>
> Thirdly, an injunction may issue pursuant to its natural power to grant injunctions conferred in respect of a particular subject matter, such as family law or trade practises law.

> Fourthly, an injunction may issue in the protection of a legal privilege or freedom. So an injunction may be obtained to prevent a person from harassing the plaintiff. Likewise even if, on the principles that have been set out here, an injunction is not otherwise obtainable to enjoying the bringing or continuation of proceedings in another court - whether in an inferior court, a court of special jurisdiction or a foreign court - it may nevertheless be obtained if the bringing or continuation of those proceedings would be unconscionable. Injunctions of these kinds may be granted whether or not inconsistent proceedings have been or will be commenced in the forum.
>
> Fifthly, an injunction (such as a Mareva injunction or freezing order) may issue in other cases in which, on miscellaneous grounds, the conduct restraint would be unconscionable. It has been said in the House of Lords that this term includes conduct which is oppressive or vexatious or which interferes with the due process of the court. Here s. 37 of the Supreme Court Act 1981 and other such provisions merely confirm the width of the court's inherent powers. "

103. Lord Scott's statement of the law is also consistent with Lord Woolf's own analysis in *Broadmoor* at [20]-[25], where he pointed out that the Court had jurisdiction in accordance with section 37(1) to enforce non-statutory public law duties by injunction, including in private law proceedings.

104. Counsel for the ISPs submitted that the Court's jurisdiction to grant an injunction was, subject to two irrelevant exceptions, limited to two situations: (i) where one party to an action can show that the other party has invaded, or threatens to invade, a legal or equitable right of the former, for the enforcement of which the latter is amenable to the jurisdiction of the Court; and (ii) where one party to an action has behaved, or threatens to behave, in a manner which is unconscionable. Although this submission receives support from dicta in some of the authorities cited in paragraph 96 above, I do not accept it. In my judgment the decisions in *Broadmoor* and *Fourie v Le Roux* show that there is no such limit on the Court's jurisdiction. It is true, that as a matter of practice, that the Court exercises its discretion in accordance with fairly well settled principles, but those principles are not immutable. On the contrary, as Lord Scott pointed out, they have evolved over time as the Court has faced new circumstances.

105. I would add three linked points. The first is that, as counsel for Richemont pointed out, Dr Spry's formulation of the first category of case in which an injunction may be granted is not restricted to injunctions against infringers of the right in question.

106. The second is that, faced with *Broadmoor* and *Fourie v Le Roux*, counsel for the ISPs submitted that there must at minimum be a prior legal or equitable or public law duty on the defendant which the grant of an injunction will enforce. Even assuming that that is correct, however, I am not persuaded that it shows that the Court has no jurisdiction to grant an injunction in circumstances such as the present. An analogy may be drawn with the equitable protective duty described by Buckley LJ in *Norwich Pharmacal Co v Customs & Excise Commissioners* [1974] AC 133 at 145-146:

> "If a man has in his possession or control goods the dissemination of which, whether in the way of trade or, possibly, merely by way of gifts (see *Upmann v Forester*, 24 Ch.D. 231) will infringe another's patent or trade mark, he becomes, as soon as he is aware of this fact, subject to a duty, an equitable duty, not to allow those goods to pass out of his possession or control at any rate in circumstances in which the proprietor of the patent or mark might be injured by infringement ensuing. The man having the goods in his possession or control must not aid the infringement by letting the goods get into the hands of those who may use them or deal with them in a way which will invade the proprietor's rights. Even though by doing so he might not himself infringe the patent or trade mark, he would be in dereliction of his duty to the proprietor. This duty is one which will, if necessary, be enforced in equity by way of injunction: see *Upmann v Elkan*, L.R. 12 Eq. 140, 7 Ch App 130."

Although this principle is inapplicable to the circumstances of the present case, it is not a long step from this to conclude that, once an ISP becomes aware that its services are being used by third parties to infringe an intellectual property right, then it becomes subject to a duty to take proportionate measures to prevent or reduce such infringements even though it is not itself liable for infringement.

107. Thirdly, both the breadth of the Court's jurisdiction under section 37(1) and the fact that the jurisdiction can be exercised in new ways are confirmed by the recent decision of the Court of Appeal in *Samsung Electronics (UK) Ltd v Apple Inc* [2012] EWCA Civ 1339, [2013] FSR 9. In that case Samsung sued Apple for a declaration of non-infringement of a Community registered design and Apple counterclaimed for infringement. Amongst the relief claimed by Apple was a publicity order under Article 15 of the Enforcement Directive. His Honour Judge Birss QC (as he then was) held that Samsung's products did not infringe Apple's design. He also made an order against Apple requiring it to publicise the decision by a notice and hyperlink on its website – a form of mandatory injunction. Apple appealed unsuccessfully against the finding of non-infringement. It also appealed against the publicity order.

108. On the question of whether this Court had jurisdiction to make the publicity order, Sir Robin Jacob, with whom Longmore and Kitchin LJJ agreed, said this:

> "70. Before I proceed however, I should first consider whether or not there is power to grant a publicity order of this sort—publicity by an intellectual property claimant that he has failed in his action for infringement. Publicity orders in intellectual property cases are quite a new thing at least in this jurisdiction. Prior to the Enforcement Directive 2004/48/EC they were, so far as I am aware, unknown here. The nearest one came to such an order was a recognition that a plaintiff could be entitled to the costs of obtaining an order for an injunction in open court even though the defendant consented for the sake of the publicity that such an order afforded, see *Fox v Luke* (1925) 43 R.P.C. 37 .

71. The Enforcement Directive changed that, providing expressly for publicity orders where the IP right holder has been successful. The purpose (Recital 27) was to act as a 'supplementary deterrent to future infringers and to contribute to the awareness of the public at large.' The Directive does not provide for publicity orders the other way round—where a party has successfully defended an unjustified claim of infringement or has obtained a declaration of non-infringement.

72. [Counsel for Samsung] accepted that the Directive was limited to publicity where an IP right holder was successful. So jurisdiction to grant the order could not stem from the Directive. [Counsel] contended that jurisdiction stemmed from s.37 of the Senior Courts Act 1981: …. The provision replaces identical legislation going back to at least the Judicature Acts of 1873–5. As is set out in *Spry on Equitable Remedies,* 7th edn (cited by Apple) the exercise of the power is not entirely unfettered. It is limited to inter alia 'the enforcement of an equitable right' and 'to restrain unconscionable conduct, such as conduct which would interfere with the due process of the court'.

73. [Counsel for Apple] did not actually contest that s.37(1) gave the court in principle a power to grant a publicity order in favour of a successful non-infringer. He referred us … to what Lord Nicholls said in *Mercedes-Benz AG v Leiduck* [1996] A.C. 284 at p.308:

> '…the jurisdiction to grant an injunction, unfettered by statute, should not be rigidly confined to exclusive categories by judicial decision. The court may grant an injunction against a party properly before it where this is required to avoid injustice, just as the statute provides and just as the Court of Chancery did before 1875. The court habitually grants injunctions in respect of certain types of conduct. But that does not mean that the situations in which injunctions may be granted are now set in stone for all time. The grant of Mareva injunctions itself gives the lie to this. As circumstances in the world change, so must the situations in which the courts may properly exercise their jurisdiction to grant injunctions. The exercise of the jurisdiction must be principled, but the criterion is injustice. Injustice is to be viewed and decided in the light of today's conditions and standards, not those of yester-year.'

…

75. I have no doubt that the court has jurisdiction to grant a publicity order in favour of a non-infringer who has been

> granted a declaration of non-infringement. A declaration is a discretionary, equitable, remedy. The injunction is an adjunct to the declaration. It will not always be appropriate to grant it. Whether or not it is depends on all the circumstances of the case—as I said earlier where there is a real need to dispel commercial uncertainty. It is that test I propose to apply here."

109. I have a number of comments to make about this passage. First, it is not binding authority, since the question of jurisdiction was not in dispute. Nevertheless, it is highly persuasive since the Court of Appeal was clearly concerned to be sure that the Court did have jurisdiction. Secondly, although the publicity order was inspired by the Enforcement Directive, it was common ground that the Enforcement Directive was not applicable. Accordingly, Sir Robin Jacob's reasoning was based upon a purely domestic interpretation of section 37(1). Thirdly, consistently with the analysis set out above, Sir Robin distinguished between the Court's power to grant an injunction and the exercise of that power. (Although Sir Robin seems to have regarded Dr Spry as saying that the exercise of the power was limited to certain situations, it can be seen from the passages quoted above that Dr Spry's analysis is entirely consistent with the passage from *Mercedes-Benz* quoted by Sir Robin which Dr Spry himself cites in support of his analysis.) Fourthly, counsel for the ISPs pointed out that Sir Robin had referred to the injunction being an adjunct to the declaration of non-infringement. Nevertheless, the entire thrust of his reasoning was that the Court had power to grant the injunction under section 37(1). In any event, the Court's power to grant a declaration is also very broad (see *Actavis UK Ltd v Eli Lilly & Co* [2014] EWHC 1511 (Pat) at [304]). Fifthly, Apple had not infringed any legal or equitable right of Samsung's. Nor did the Court of Appeal find that Apple had acted unconscionably. Rather, the essence of the Court's reasoning was that, having created commercial uncertainty in the market, Apple had come under a duty to take reasonable steps to correct that state of affairs. That was a duty which could be enforced by the grant of an injunction.

110. What the three points mentioned above show is that, not only does the Court have jurisdiction to grant a website blocking injunction against an ISP in a trade mark case, but also there is a principled basis upon which the Court may exercise that jurisdiction.

111. Accordingly, I conclude that, upon a purely domestic interpretation of section 37(1), the Court has jurisdiction to grant the orders sought by Richemont and that there is a principled basis for it to do so. In case I am wrong about that, however, I shall go on to consider whether, assuming the Court has no such power upon a purely domestic interpretation of section 37(1), section 37(1) should be interpreted in accordance with the third sentence of Article 11 of the Enforcement Directive as conferring such a power. Before doing so, it is necessary to say a little more about the way in which Article 8(3) of the Information Society Directive and Article 11 of the Enforcement Directive were implemented in the UK.

Implementation of Article 8(3) of the Information Society Directive and Article 11 of the Enforcement Directive

112. The Government implemented both the Information Society Directive and the Enforcement Directive by passing secondary legislation where that was considered

appropriate. In both cases, the secondary legislation included amendments to primary legislation, using the power conferred by section 2(2) of the European Communities Act 1972.

113. When considering implementation of Article 8(3) of the Information Society Directive, the Government initially thought that it did not need to take any action. When consulting on its implementation proposals in *EC Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society: Consultation Paper on Implementation of the Directive in the United Kingdom* (Patent Office, 7 August 2002), the Government stated at 16:

> "Regarding Article 8.3, it is already possible under UK law to seek injunctions against intermediaries. It is also possible to notify an intermediary of an injunction served on an infringer so that the intermediary is liable for contempt of court proceedings if he aids and abets an infringer. It is considered that this meets the requirements of Article 8.3."

114. It is not clear on what basis the Government considered that it was "already possible under UK law to seek injunctions against intermediaries". All one can say is that no express reference was made to section 37(1) of the 1981 Act.

115. After the consultation, however, the Government changed its mind. In *Consultation on UK Implementation of Directive 2001/29/EC on Copyright and Related Rights in the Information Society: Analysis of Responses and Government Conclusions* (Patent Office, 2003), it stated:

> "8.3 The consultation paper suggested that no specific action might be needed to implement Article 8.3, requiring that right owners be able to apply for injunctions against intermediaries whose services are used by third-parties to infringe rights, on the basis that it is already possible to seek such injunctions under common law in the UK. Right owner organisations generally expressed strong concern that, unless specific provision is made to implement Article 8.3, there would be uncertainty as to whether right owners can apply for injunctions, the more so because the Article 5.1 exception means that intermediaries will not themselves be infringing rights in the circumstances set out in that article. Some representatives of internet service providers, the main 'intermediaries' to whom A.8.3 relates, also sought clarity as to the position.
>
> 8.4 On further consideration, the Government has concluded that, in order to avoid uncertainty, Article 8.3 should be specifically implemented in UK law, by way of provisions in Parts I & II of the CDPA enabling the High Court (or Court of Session in Scotland) to grant injunctions against service providers, where the latter have actual knowledge of a third party using the service to infringe rights. …"

116. When considering implementation of Article 11 of the Information Society Directive, the Government again took the view that it did not need to take any action. When consulting on its implementation proposals in *Consultation Paper: The UK*

*Implementation of the Directive on the Enforcement of Intellectual Property Rights (*Patent Office, August 2005), it stated in relation to Article 11:

> "**No action is required.**
>
> The jurisdiction of the High Court to grant injunctions is derived from **section 37(1) of the Supreme Court Act 1981**. It may do so on such terms and conditions as it thinks fit (**Section 37(2)**).
>
> …
>
> A final injunction is usually granted to an intellectual property right holder who proves at trial that his rights have been infringed by the defendant (*Chiron v Organon (No 10)* [1995] FSR 325 (as a general rule a defendant who interferes with a proprietary right will be injuncted).
>
> (see earlier comments about intermediaries)."

117. Read in isolation, this would appear to indicate that the Government thought that section 37(1) enabled the High Court to grant injunctions against intermediaries as required by the third sentence of Article 11. The reference to "earlier comments about intermediaries", however, refers to the section of the document discussing implementation of Article 9(1)(a). This section notes that Article 9(1)(a) requires member states "to ensure that the court may … issue an interlocutory injunction against an alleged infringer to prevent a threatened infringement" and adds "(This includes against an intermediary whose services are being used to infringe an intellectual property[11])". Footnote 11 states:

> "This wording in the Article repeats that found in Article 8(3) of Directive on the harmonisation of copyright and related rights in the information society11 [*sic*]. Article 8(3) was implemented by section 97A of the Copyright and Related Rights Regulation 200311 [*sic*]. Section 97A provides that the High Court shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright …"

This section of the document also states:

> "**No action is required.**
>
> The **Supreme Court Act 1981**, section 37 states that the High Court may, by order, whether interlocutory or final grant an injunction in all cases in which it is just and convenient to do so.
>
> …

> The court is only able to issue an interim injunction against a person against whom a cause of action exists. The following are the persons against whom a cause of action will exist and injunction may be made:
>
> [Separate lists for copyright, patents, trade marks, design right and registered designs]".

118. Even leaving aside the typographical errors in footnote 11, this is very confused, for a number of reasons. First, the requirement to provide for a final injunction against intermediaries comes from the third sentence of Article 11 of the Enforcement Directive, whereas Article 9(1)(a) only requires provision for an interim injunction. Secondly, the consultation paper states that the court is only able to issue an interim injunction against a person against whom a cause of action exists, but does not suggest that a copyright or trade mark owner would have a cause of action against an intermediary which was not itself infringing the relevant right. Thirdly, the consultation paper notes that Article 8(3) of the Information Society Directive was implemented by section 97A of the 1988 Act, but offers no explanation as to why, if section 97A was required in cases involving copyright and related rights, no similar provision is required in cases involving other intellectual property rights.

119. It appears that none of the responses to the consultation paper changed the Government's thinking on this point. Accordingly, no statutory provision corresponding to section 97A of the 1988 Act was introduced with regard to intellectual property rights other than copyright and related rights.

120. Counsel for the ISPs submitted that the consultation paper does not show that the Government had a clear understanding that section 37(1) of the 1981 Act empowered the High Court to grant an injunction against intermediaries who were not themselves infringers. I accept that, but it does show that the Government believed that existing domestic law complied with the third sentence of Article 11 and therefore nothing needed to be done to implement it. Certainly, there was no intention on the part of the Government not to implement the third sentence of Article 11.

Interpretation of section 37(1) in accordance with the third sentence of Article 11

121. The question of whether the Court had jurisdiction under section 37(1) to grant an injunction against an intermediary which was not itself an infringer arose in *L'Oréal SA v eBay International AG* [2009] EWHC 1094 (Ch), [2009] RPC 21. In that case, L'Oréal contended that, having established a number of infringements of their trade marks by the fourth to tenth defendants, the third sentence of Article 11 of the Enforcement Directive required this Court to grant an injunction against eBay to prevent the same or similar infringements in the future even if eBay were not themselves liable for trade mark infringement. eBay disputed this.

122. So far as domestic law was concerned, having considered a number of authorities (but not *Fourie v Le Roux*) at [447]-[454], I concluded that, if the third sentence of Article 11 required the grant of an injunction to prevent future infringements against an intermediary who was not an infringer, then that provided a sufficient reason for a court of equity to exercise its power to grant an injunction to protect an intellectual property right which has been infringed. In saying that, I was not treating Article 11

as having direct effect, but as providing a principled basis for the exercise of an existing jurisdiction in a new way. The question then was what the third sentence of Article 11 required.

123. Having considered that question at [455]-[465], I concluded that it was a matter upon which the guidance of the CJEU was required. Accordingly, I referred the following question to the CJEU, which is question 10 of the questions referred in that case:

> "Where the services of an intermediary such as an operator of a website have been used by a third party to infringe a registered trade mark, does Article 11 …. require Member States to ensure that the trade mark proprietor can obtain an injunction against the intermediary to prevent further infringements of the said trade mark, as opposed to continuation of that specific act of infringement, and if so what is the scope of the injunction that shall be made available?"

124. The CJEU considered this question in its judgment in Case C-324/09 [2011] ECR I-6011 at [125]-[144]. At [128]-[130] the Court held that the injunction referred to in the third sentence of Article 11 could not be equated with the injunction aimed at prohibiting the continuation of the infringement referred to in the first sentence. At [131]-[134] the Court held that consideration of the objective pursued by the Enforcement Directive, and of Article 18 of the E-Commerce Directive and recital (24) of the Enforcement Directive, led to the conclusion that the jurisdiction conferred by the third sentence of Article 11 was not limited to bringing infringements to an end, but extended to preventing further infringements. At [135]-[138] the Court held that the rules relating to the conditions to be met and the procedure to be followed to obtain injunctions under the third sentence of Article 11 were a matter for national law, but that the rules must be both designed and applied in such a manner that the measures were effective and dissuasive, and observed the limitations of the Enforcement Directive and the sources of law to which it referred. For present purposes, the Court's statement at [137] is particularly pertinent:

> "… in view of the fact, stated in the order for reference and referred to at paragraph 24 of this judgment, that the United Kingdom has not adopted specific rules to implement the third sentence of Article 11 …, the referring court will, when applying national law, be required to do so, as far as possible, in the light of the wording and the purpose of the third sentence of Article 11 (see, by analogy, Case C-106/89 *Marleasing* [1990] ECR I-3135, paragraph 8, Joined Cases C-378/08 to C-380/07 *Angelidaki and Others* [2009] ECR I-3071, paragraph 106)."

125. The Court went on at [139]-[143] to hold that the measures required of an online service provider by such an injunction could not consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website, nor could an injunction have as its object or effect a general and permanent prohibition on the selling, via that website, of goods bearing the trade marks in question. Nevertheless, measures such as requiring the provider to suspend perpetrators of infringements or to identify

perpetrators acting in the course of trade could be granted. All such measures had to strike a fair balance between the interests involved. Accordingly, the Court concluded at [144]:

> "In view of the foregoing, the answer to the tenth question is that the third sentence of Article 11 of Directive 2004/48 must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, dissuasive and must not create barriers to legitimate trade."

126. The litigation between L'Oréal and eBay was subsequently settled, and so I was not called upon to apply this guidance to the facts of that case.

127. It seems to me to be plain from the judgment of the CJEU in *L'Oréal v eBay*, and in particular what it said at [137], that section 37(1) should, if possible, be interpreted as empowering the Court to grant an injunction against an intermediary who is not an infringer so as to comply with the third sentence of Article 11. On the face of it, there is no difficulty in interpreting section 37(1) in that manner. On the contrary, the wording of section 37(1) is extremely broad and, interpreted literally, does precisely that.

128. Counsel for the ISPs submitted that it was not possible to construe section 37(1) consistently with the third sentence of Article 11 for four reasons. First, because the third sentence of Article 11 does not have horizontal effect. This is true, but irrelevant. The absence of horizontal effect does not affect the *Marleasing* principle.

129. The second reason was that Parliament had chosen not to transpose the third sentence of Article 11 with respect to intellectual property rights other than copyright and related rights. For the reasons given in paragraphs 116-120 above, however, this is not a correct statement of the position. It is true that the Government did not promulgate secondary legislation to implement the third sentence of Article 11, but this was because it believed that this was not necessary. It is also true that it is difficult to see why the Government took a different view to that which it had ultimately taken when implementing Article 8(3) of the Information Society Directive (or why, having taken that view, it did not repeal sections 97A and 191JA of the 1988 Act), but this does not matter.

130. The third reason is that it is not possible for the Court to enlarge its powers under section 37(1) absent an Act of Parliament. This misses the point, however. Even if section 37(1) would otherwise be construed as the ISPs contend, Parliament has passed an Act, the European Communities Act 1972, which, as is well established, gives primacy to EU law. Thus it is pursuant to the 1972 Act that the *Marleasing* principle comes into play.

131. The fourth reason is that creating a new remedy for trade mark infringement would go against the grain of the Trade Marks Act 1994, in particular because it is not provided for by sections 2(1), 9(1) or 14. But the 1994 Act both confers remedies against persons who are not necessarily infringers (as can be seen from section 16(1)) and yet does not purport to contain a comprehensive code of the remedies available to a trade mark proprietor (as can be seen from section 16(4)). More generally, there is nothing inconsistent between granting an injunction against intermediaries under section 37(1) and the provisions of the 1994 Act, just as there is nothing inconsistent between the third sentence of Article 11 and the Trade Marks Directive.

132. Accordingly, I conclude that, even if the Court would not have power to grant a website blocking injunction in a trade mark case upon a purely domestic interpretation of section 37(1), section 37(1) can and should be interpreted in compliance with the third sentence of Article 11 by virtue of the *Marleasing* principle. If it were otherwise, the UK would be in breach of its obligations under the Directive.

Provided for by law?

133. It is common ground that the orders sought by Richemont would amount to a limitation on the ISPs' rights under Article 16, and on their subscribers' rights under Article 11, of the Charter. Article 52(1) of the Charter requires that any limitation on the exercise of the rights and freedoms must be "provided for by law". This is the same requirement as the requirement under Article 10(2) of the European Convention on Human Rights that restrictions on freedom of expression must be "prescribed by law". Counsel for the ISPs submitted that, if section 37(1) of the 1981 Act were to be construed as enabling the Court to grant orders of the kind sought by Richemont, it would not comply with this requirement.

134. In support of this submission, counsel for the ISPs relied in particular on the Concurring Opinion of Judge Pinto de Albuquerque in the decision of the Second Section of the European Court of Human Rights in *Yildirim v Turkey* (Application No. 3111/10, 18 December 2012). In his Concurring Opinion Judge Pinto suggested that there were no fewer than 11 "minimum criteria for Convention-compatible legislation on Internet blocking measures", and that in addition this framework must be established by "specific legal provisions; neither the general provisions and clauses governing civil and criminal responsibility nor the e-commerce Directive constitute a valid basis for ordering Internet blocking".

135. I do not accept this submission, for the following reasons. First, the majority judgment of the Second Section in *Yildirim v Turkey* does not go as far as Judge Pinto. The majority judgment held at [57] that the test to be applied was as follows:

> "The Court reiterates at the outset that the expression 'prescribed by law', within the meaning of Article 10 § 2, requires firstly that the impugned measure should have some basis in domestic law; however, it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences, and that it should be compatible with the rule of law (see, among many other authorities, *Dink v. Turkey*, nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, § 114, 14

> September 2010). According to the Court's established case-law, a rule is 'foreseeable' if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see, among many other authorities, *RTBF v. Belgium*, no. 50084/06, § 103, ECHR 2011, and *Altuğ Taner Akçam v. Turkey*, no. 27520/07, § 87, 25 October 2011)."

See also *Delfi v Estonia* (2014) 58 EHRR 29 at [71]-[72].

136. On the facts of the *Yildirim* case, the majority held this requirement was not satisfied because: (i) the measure in question consisted of wholesale blocking of all Google Sites, which incidentally resulted in blocking of the applicant's website; (ii) the measure was a prior restraint imposed before a ruling had been given on the merits; (iii) the measure was imposed by an administrative body; (iv) the purpose of the measure was to block access to a specific offending website, but no attempt had been made by the national authorities to weigh up the competing interests at stake; (v) the measure produced arbitrary effects; and (vi) the judicial review procedures available were insufficient to avoid abuse. This reasoning does not suggest that the mere fact that the legislation is general rather than specific means that it is not prescribed by law.

137. Secondly, I do not understand even Judge Pinto to have gone so far as to say that website blocking orders made pursuant to Article 8(3) of the Information Society Directive and the third sentence of Article 11 of the Enforcement Directive would not be "prescribed by law", at least if the orders complied with the other requirements of EU law. Accordingly, provided that section 37(1) is interpreted and applied in accordance with the third sentence of Article 11, and the other requirements of EU law, it does not appear to me that even Judge Pinto would regard it as falling foul of this requirement.

138. Thirdly, I considered the question whether the order sought on the first section 97A application was "prescribed by law" in *20C Fox v BT* at [163]-[177]. I concluded that the order fell well within the range of orders which were foreseeable by ISPs on the basis of section 97A, and still more Article 8(3) of the Information Society Directive, and thus was "prescribed by law". I adhere to that conclusion, which does not appear to be undermined by any of the subsequent case law of the CJEU or the ECtHR that has been drawn to my attention. In my judgment, the orders sought by Richemont in the present case fall within the range of orders which were foreseeable by ISPs on the basis of section 37(1), at least if it is interpreted and applied in accordance with the third sentence of Article 11 and the other requirements of EU law. Section 37(1) also satisfies the requirements of accessibility and compatibility with the rule of law laid down by the ECtHR. Accordingly, I conclude that the orders sought by Richemont are "prescribed by law" and "provided for by law".

Threshold conditions for the exercise of the jurisdiction

139. Where an injunction is against an intermediary on the basis that its services have been used to infringe copyright or related rights, Parliament has laid down a number of threshold conditions for the exercise of the High Court's jurisdiction to grant an injunction. In the context of website blocking orders, it can be seen from the cases

cited in paragraph 3 above that there are four conditions which must be satisfied. First, that the defendant is a service provider. Secondly, that users and/or the operator of the website in question infringe the claimant's copyrights. Thirdly, that users and/or the operator of the website use the defendant's services to do that. Fourthly, that the defendant has actual knowledge of this.

140. For the reasons discussed above, Parliament has not laid down any threshold conditions for the exercise of the High Court's jurisdiction to grant an injunction against an intermediary on the basis that its services have been used to infringe other intellectual property rights. Having regard to the analysis of section 37(1) of the 1981 Act above, this might be thought to lead to the conclusion that the Court's discretion is entirely unfettered. In my judgment, however, it is clear from the judgments of the CJEU in *L'Oréal v eBay* and other cases that this is not correct. On the contrary, the Court must exercise its power under section 37(1) consistently with the provisions of the Enforcement Directive, and in particular Article 3 and the third sentence of Article 11, and with other applicable provisions of EU law, and in particular Articles 12 to 15 of the E-Commerce Directive.

141. In my judgment, it follows that similar threshold conditions must be satisfied in order for a website blocking injunction to be granted in a trade mark case. First, the ISPs must be intermediaries within the meaning of the third sentence of Article 11. Secondly, either the users and/or the operators of the website must be infringing the claimant's trade marks. Thirdly, the users and/or the operators of the website must use the ISPs' services to do that. Fourthly, the ISPs must have actual knowledge of this. Each of the first three conditions follows from the wording of Article 11 itself. The fourth condition is not contained in Article 11, but in my view it follows from Article 15 of the E-Commerce Directive and by analogy with Articles 13(1)(e) and 14(1)(a) of the E-Commerce Directive. If ISPs could be required to block websites without having actual knowledge of infringing activity, that would be tantamount to a general obligation to monitor. It is also difficult to see that such a requirement would be consistent with the requirements of Article 3(1) of the Enforcement Directive. As to what constitutes "actual knowledge" in this context, I see no reason to interpret this requirement differently to the manner in which I interpreted it in the section 97A/Article 8(3) context: see *20C Fox v BT* at [114]-[157].

Are the threshold conditions satisfied in the present case?

Are the ISPs intermediaries?

142. There is no dispute that each of the ISPs is an intermediary within the meaning of Article 11 of the Enforcement Directive.

Are the operators of the Target Websites infringing the Trade Marks?

143. There is no dispute that the operators of the Target Websites are infringing the Trade Marks. It is nevertheless necessary for me to explain why this is the case, since it bears on the third condition.

144. The case law of the CJEU establishes that the proprietor of a trade mark can only succeed in a claim under Article 5(1)(a) of the Directive if six conditions are satisfied: (i) there must be use of a sign by a third party within the relevant territory; (ii) the use

must be in the course of trade; (iii) it must be without the consent of the proprietor of the trade mark; (iv) it must be of a sign which is identical to the trade mark; (v) it must be in relation to goods or services which are identical to those for which the trade mark is registered; and (vi) it must affect or be liable to affect the functions of the trade mark: see in particular Case C-206/01 *Arsenal Football plc v Reed* [2002] ECR I-10273 at [51], Case C-245/02 *Anheuser-Busch Inc v Budějovický Budvar np* [2004] ECR I-10989 at [59], Case C-48/05 *Adam Opel AG v Autec AG* [2007] ECR I-1017 at [18]-[22], Case C-17/06 *Céline SARL v Céline SA* [2007] ECR I-7041 at [16] and Case C-62/08 *UDV North America Inc v Brandtraders NV* [2009] ECR I-1279 at [42].

145. Richemont contend that the operators of the Target Websites infringe the Trade Marks in two main ways. First, by using signs identical to the Trade Marks in respect of goods identical to those for which the Trade Marks are registered in advertising, and by offering such goods under those signs, on the Target Websites themselves. Secondly, by selling goods bearing such signs in response to orders. In both cases the use is in respect of counterfeit goods and is without Richemont's consent.

146. There can be no dispute that in each case conditions (ii)-(iv) are satisfied. So far as condition (i) is concerned, it is clear that each of the Target Websites is advertising and offering the goods in a manner that is targeted at consumers in the UK as required by the jurisprudence of the CJEU: see in particular *L'Oréal v eBay* at [61]-[65]. In the case of the sales, it is immaterial that the goods are dispatched from outside the EU to consumers within the EU: see Case C-98/13 *Blomqvist v Rolex SA* [EU:C:2014:55], [2014] ETMR 25. As to condition (vi), both kinds of use complained of by Richemont are liable adversely to affect the origin function of the Trade Marks. This so even where the Target Websites make it clear that the goods are replicas, since that does not exclude the likelihood of post-sale confusion: see *Arsenal v Reed*.

Do the operators of the Target Websites use the ISPs' services to infringe?

147. Counsel for the ISPs submitted that it was unclear that the operators of the Target Websites used the ISPs' services to infringe the Trade Marks and suggested that this was a matter on which guidance from the CJEU was required. As she pointed out, the CJEU has addressed this question in two cases concerning copyright and related rights, but has not yet considered it in the context of rights such as trade marks.

148. The first case was Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-1227. In that case LSG was a collecting society which enforced the rights of recorded music producers in their sound recordings and the rights of the recording artists in respect of the exploitation of those recordings in Austria, in particular the right to reproduce and distribute the recordings and the right to make them available to the public. Tele2 was an ISP (or "access provider") which assigned to its clients IP addresses, which were usually dynamic rather than static. Tele2 was able to identify individual clients on the basis of the IP address and the period or date when it was assigned. The rightholders were suffering financial loss as a result of the creation of file-sharing systems which make it possible for participants to exchange copies of recordings. In order to be able to bring civil proceedings against the perpetrators, LSG applied for an order requiring Tele2 to disclose the names and addresses of persons to

whom it had provided an Internet access service and whose IP addresses, together with the day and time of the connection, were known.

149. The Oberster Gerichtshof (Austrian Supreme Court) referred two questions to the CJEU, the first of which was as follows:

> "Is the term 'intermediary' in Article 5(1)(a) and Article 8(3) of Directive [2001/29] to be interpreted as including an access provider who merely provides a user with access to the network by allocating him a dynamic IP address but does not himself provide him with any services such as email, FTP or file-sharing services and does not exercise any control, whether *de iure* or *de facto*, over the services which the user makes use of?"

150. Tele2 argued that it was not an "intermediary" for reasons which the Court summarised at [38] as follows:

> "Tele2 maintains, inter alia, that intermediaries must be in a position to bring copyright infringements to an end. Internet access providers, on the other hand, in as much as they exercise no control, whether *de iure* or *de facto*, over the services accessed by the user, are not capable of bringing such infringements to an end and, accordingly, are not 'intermediaries' within the meaning of Directive 2001/29."

151. The Court rejected this argument for the following reasons:

> "42. … under Article 8(3) of Directive 2001/29, Member States are to ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.
>
> 43. Access providers who merely enable clients to access the Internet, even without offering other services or exercising any control, whether *de iure* or *de facto*, over the services which users make use of, provide a service capable of being used by a third party to infringe a copyright or related right, inasmuch as those access providers supply the user with the connection enabling him to infringe such rights.
>
> 44. Moreover, according to Recital 59 in the preamble to Directive 2001/29, rightholders should have the possibility of applying for an injunction against an intermediary who 'carries a third party's infringement of a protected work or other subject-matter in a network'. It is common ground that access providers, in granting access to the Internet, make it possible for such unauthorised material to be transmitted between a subscriber to that service and a third party.

> 45. That interpretation is borne out by the aim of Directive 2001/29 which, as is apparent in particular from Article 1(1) thereof, seeks to ensure the legal protection of copyright and related rights in the framework of the internal market. The protection sought by Directive 2001/29 would be substantially diminished if 'intermediaries', within the meaning of Article 8(3) of that directive, were to be construed as not covering access providers, which alone are in possession of the data making it possible to identify the users who have infringed those rights.
>
> 46 In view of the foregoing, the answer to the first question is that access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether *de iure* or *de facto*, over the services which users make use of, must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29."

152. The second case is Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* [EU:C:2014:192], [2014] Bus LR 541. In that case UPC was a major Austrian ISP (or "access provider"). Constantin and Wega were the owners of copyrights in various films. These films, along with many other copyrighted films, were made available without Constantin's or Wega's consent on a website called kino.to. I understand that kino.to was one of the most popular websites for the streaming and downloading of copyrighted film and TV content in German-speaking territories, with a top 40 ranking on Alexa.com, prior to being taken down upon the apprehension of its operators by the German authorities following an investigation spanning several years.

153. On an application by Constantin and Wega, the Court of First Instance made an order requiring UPC to block access to kino.to. That order was upheld by the Court of Appeal. UPC appealed to the Oberster Gerichtshof, which referred four questions to the CJEU concerning the proper interpretation of Article 8(3) of the Information Society Directive. The first question was as follows:

> "Is Article 8(3) of Directive 2001/29/EC (the Information Society Directive) to be interpreted as meaning that a person who makes protected subject matter available on the internet without the rightholder's consent (Article 3(2) of the Information Society Directive) is using the services of the access providers of persons seeking access to that protected subject matter?"

154. The Court answered this question in the affirmative for the following reasons:

> "31. Having regard to the objective pursued by Directive 2001/29, as shown in particular by Recital 9 thereof, which is to guarantee rightholders a high level of protection, the concept of infringement thus used must be understood as including the case of protected subject-matter placed on the internet and

made available to the public without the agreement of the rightholders at issue.

32. Accordingly, given that the internet service provider is an inevitable actor in any transmission of an infringement over the internet between one of its customers and a third party, since, in granting access to the network, it makes that transmission possible (see, to that effect, the order in Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* [2009] ECR I-1227, paragraph 44), it must be held that an internet service provider, such as that at issue in the main proceedings, which allows its customers to access protected subject-matter made available to the public on the internet by a third party is an intermediary whose services are used to infringe a copyright or related right within the meaning of Article 8(3) of Directive 2001/29.

33. Such a conclusion is borne out by the objective pursued by Directive 2001/29. To exclude internet service providers from the scope of Article 8(3) of Directive 2001/29 would substantially diminish the protection of rightholders sought by that directive (see, to that effect, order in *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, paragraph 45).

34. That conclusion cannot be called into question by the argument that, for Article 8(3) of Directive 2001/29 to be applicable, there has to be a contractual link between the internet service provider and the person who infringed a copyright or related right.

35. Neither the wording of Article 8(3) nor any other provision of Directive 2001/29 indicates that a specific relationship between the person infringing copyright or a related right and the intermediary is required. Furthermore, that requirement cannot be inferred from the objectives pursued by that directive, given that to admit such a requirement would reduce the legal protection afforded to the rightholders at issue, whereas the objective of that directive, as is apparent inter alia from Recital 9 in its preamble, is precisely to guarantee them a high level of protection.

36. Nor is the conclusion reached by the Court in paragraph 30 of this judgment invalidated by the assertion that, in order to obtain the issue of an injunction against an internet service provider, the holders of a copyright or of a related right must show that some of the customers of that provider actually access, on the website at issue, the protected subject-matter made available to the public without the agreement of the rightholders.

> 37. Directive 2001/29 requires that the measures which the Member States must take in order to conform to that directive are aimed not only at bringing to an end infringements of copyright and of related rights, but also at preventing them (see, to that effect, Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, paragraph 31, and Case C-360/10 *SABAM* [2012] ECR, paragraph 29).
>
> 38. Such a preventive effect presupposes that the holders of a copyright or of a related right may act without having to prove that the customers of an internet service provider actually access the protected subject-matter made available to the public without their agreement.
>
> 39. That is all the more so since the existence of an act of making a work available to the public presupposes only that the work was made available to the public; it is not decisive that persons who make up that public have actually had access to that work or not (see, to that effect, Case C-306/05 *SGAE* [2006] ECR I-11519, paragraph 43)."

155. Counsel for the ISPs argued that the Court's reasoning in these cases could not simply be translated to the present case. I disagree. In my judgment the principles articulated by the CJEU in these passages are readily applicable to the situation at hand. As discussed above, the operators of the Target Websites are infringing the Trade Marks by placing on the internet advertisements and offers for sale which are targeted at UK consumers. The ISPs have an essential role in these infringements, since it is via the ISPs' services that the advertisements and offers for sale are communicated to 95% of broadband users in the UK. It is immaterial that there is no contractual link between the ISPs and the operators of the Target Websites. It is also immaterial that UK consumers who view the Target Websites may not purchase any goods, since the first type of infringement is already complete by then. It is also immaterial that, if a UK consumer does purchase an item, the item will be transported by courier or post, since the contract of sale will be concluded via the website.

156. Counsel for the ISPs also pointed out that Richemont's evidence did not specifically establish that the Target Websites had been accessed via any of the ISPs' services. Counsel for Richemont answered this point by demonstrating in court that it was possible to access one of the Target Websites via BT's service. I am satisfied that the same is true of the other Target Websites and the other ISPs.

Do the ISPs have actual knowledge of this?

157. There is no dispute that, if the operators of the Target Websites use the ISPs' services to infringe, then the ISPs have actual knowledge of this. They have acquired such knowledge in two ways. First, on 17 March 2014 Richemont sent the ISPs emails attaching two schedules, one containing information about the Trade Marks and the other information about the test purchases from each of the Target Websites. Secondly, as a result of being served with Richemont's evidence in support of the present application.

Principles to be applied

158. Counsel for the ISPs submitted that the Court should only grant the orders sought by Richemont if the following requirements were satisfied:

i) the relief must be necessary;

ii) the relief must be effective;

iii) the relief must be dissuasive;

iv) the relief must not be unnecessarily complicated or costly;

v) the relief must avoid barriers to legitimate trade;

vi) the relief must be fair and equitable and strike a "fair balance" between the applicable fundamental rights; and

vii) the relief must be proportionate.

159. I shall consider these suggested requirements in turn.

Necessary

160. Article 3(1) of the Enforcement Directive states that "Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of … intellectual property rights". Article 52(1) of the Charter states "… limitations may be made only if they are necessary …".

161. Counsel for the ISPs submitted that these provisions meant that Richemont had to show that the orders sought were necessary to ensure the enforcement of the Trade Marks. She further submitted that, although this did not mean that a blocking injunction must be the measure of last resort, it did mean that Richemont had to show that blocking was the least onerous measure that could achieve an equivalent level of protection.

162. I did not understand counsel for the ISPs to be submitting that it was incumbent on Richemont to show that the orders sought are necessary to ensure the enforcement of the Trade Marks in the sense that they are indispensable for that purpose, but if that was her submission I would reject it. Article 3(1) of the Enforcement Directive is directed to the Member States. It requires Member States to make available to rightholders the range of remedies which is necessary to combat infringement of intellectual property rights. This includes injunctions in accordance with the third sentence of Article 11. As discussed above, the UK complies with this by virtue of section 37(1) of the 1981 Act. Article 3(2) goes on to require that such remedies shall be proportionate. As for Article 52(1), what this means is that the rights protected by the Charter can only be restricted where this is necessary to protect other rights protected by the Charter. Where two rights, or sets of rights, are in conflict, then the conflict must be resolved by applying the principle of proportionality to each and striking a balance between them. For both reasons, it must be shown that the orders are proportionate. As I shall discuss below, I accept that, when assessing whether the orders are proportionate, the court is required to consider whether alternative

measures are available which are less onerous. Accordingly, I shall carry out that exercise in the context of assessing the proportionality of the orders.

Effective

163. Article 3(2) of the Enforcement Directive requires that remedies for the enforcement of intellectual property rights must be "effective". Similar language is to be found in Article 19(1) of the Treaty on European Union and in Article 41(1) of TRIPS. Counsel for the ISPs submitted that the corollary of this requirement was that a remedy should not be granted if it would not be effective. She further submitted that it was incumbent on Richemont to show that the orders would be likely to achieve a significant reduction in the overall levels of access to infringing content, although she accepted that Richemont did not have to show that the orders would be 100% effective to prevent access to the Target Websites.

164. Article 3(2) requires Member States to make available remedies for infringement of intellectual property rights which are effective, that is to say, effective (among other things) to prevent further infringements. I accept that it is pointless to grant a remedy which will be wholly ineffective. I do not accept that it follows that it is incumbent on the rightholder to demonstrate that the remedy sought will be effective in reducing the overall level of infringement of its intellectual property right(s).

165. This issue has been addressed in two recent decisions. The first in time is that of the Gerechtshof 's-Gravenhage (Court of Appeal of The Hague) in *Ziggo BV v Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN)* (28 January 2014). BREIN was a collecting society which sought orders against two large Dutch ISPs, Ziggo and XS4ALL, requiring them to block access to TPB pursuant to the Dutch legislation which implemented Article 8(3) of the Information Society Directive. On 12 January 2012 the Rechtbank s'Gravenhage (District Court of The Hague) granted the orders sought. On 10 May 2012 BREIN obtained preliminary injunctions in similar terms against the other four major Dutch ISPs. Ziggo and XS4ALL's appeal was allowed by the Court of Appeal, although a further appeal by BREIN to the Hoge Raad (Dutch Supreme Court) is pending.

166. In section 4 of its judgment, the Court of Appeal considered whether the users or operators of TPB used Ziggo and XS4ALL's services to infringe the rights administered by BREIN. It concluded that Ziggo and XS4ALL's subscribers did so, but that the operators of TPB only did so in relation to the artwork of CDs and DVDs etc and not the actual sound recordings and films etc. I note that this is contrary to the conclusion I reached in *Dramatico v Sky* (and see most recently *Paramount v Sky* and *Paramount v Sky 2*). Counsel for Richemont submitted that the Court of Appeal's treatment of the question of efficacy had to be seen in the light of its conclusions on infringement. In principle this must be correct, since the Court of Appeal went on to give separate consideration to the proportionality of the orders with respect to the infringements concerning artwork and its reasoning was somewhat different to its reasoning in relation to the works, but I am not sure that this was key to the decision.

167. In section 5 of its judgment, the Court of Appeal considered the question of proportionality. The Court accepted that the evidence showed that the number of visits to TPB had significantly decreased after the blocking orders were granted. Despite this, the Court of Appeal held that the orders were not effective and therefore

were not proportionate. The Court concluded at [5.13] to [5.22] that the evidence showed that the blocking orders had not reduced the *overall* level of infringement. This was for three main reasons: first, some users had circumvented the blocking orders; secondly, other users had used alternative BitTorrent websites; and thirdly, while some users had made fewer illegal downloads, other users had increased their downloading activity. It reached this conclusion in the light, in particular, of a report from the Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek or TNO (Netherlands Organisation for Applied Scientific Research) analysing network information supplied by XS4ALL and a paper discussing a study carried out by academics from the Institute of Information Law in Amsterdam and elsewhere (this paper has subsequently been published: see J. Poort *et al*, "Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay", *Telecommunications Policy* 38 (2014) 383-392.) So far as the question of the use of the alternative BitTorrent websites was concerned, the Court of Appeal also held at [5.23] to [5.24] that BREIN was not justified in making a first application against TPB as a test case and planning to make applications against TPB's principal competitors subsequently, and should have filed applications against all the principal sites together.

168. The second case is *UPC v Constantin*. In that case Constantin and Wega had applied for a bar on UPC "facilitating access" to kino.to by way of a general "prohibition of outcome". Such a "prohibition of outcome" was a standard order under the Austrian law relating to infringements of absolute rights. If such an order was made, there would not be any examination as to whether complete blocking was possible at all or whether the measures required for this adequately took account of the fundamental rights of the parties involved and were proportionate until there were enforcement proceedings for breach of the order. The Oberster Gerichtshof was concerned that an examination of fundamental rights and proportionality only after the event in enforcement proceedings failed to meet the requirements of EU law. Accordingly, question 3 of the reference was as follows:

> "If the answer to the first question or the second question is in the affirmative and an injunction is therefore to be issued against the user's access provider in accordance with Article 8(3) of the Information Society Directive: is it compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to prohibit an access provider from allowing its customers access to a certain website (without ordering specific measures) as long as the material available on that website is provided exclusively or predominantly without the rightholder's consent, if the access provider can avoid incurring preventive penalties for breach of the prohibition by showing that it had nevertheless taken all reasonable measures?"

169. When answering this question, the CJEU stated the applicable principles as follows:

> "45. In order to assess whether an injunction such as that at issue in the main proceedings, taken on the basis of Article 8(3) of Directive 2001/29, is consistent with EU law, it is … necessary to take account in particular of the requirements that stem from

> the protection of the applicable fundamental rights, and to do so in accordance with Article 51 of the Charter of Fundamental Rights of the European Union ('the Charter') (see, to that effect, *Scarlet Extended*, paragraph 41).
>
> 46. The Court has already ruled that, where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order. Then, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but also ensure that they do not rely on an interpretation of it which would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality (see, to that effect, Case C-275/06 *Promusicae* [2008] ECR I-271, paragraph 68).
>
> 47. In the present case, it must be observed that an injunction such as that at issue in the main proceedings, taken on the basis of Article 8(3) of Directive 2001/29, makes it necessary to strike a balance, primarily, between (i) copyrights and related rights, which are intellectual property and are therefore protected under Article 17(2) of the Charter, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter."

170. So far as the ISP's freedom to conduct a business was concerned, the Court of Justice held at [48]-[54] that, while such an injunction restricted that freedom, in particular because it obliged the addressee to take measures which might represent a significant cost for him, it did not seem to infringe the very substance of that freedom, because it left the addressee to determine the specific measures to be taken to achieve the result sought and allowed the addressee to avoid liability by proving he had taken all reasonable measures.

171. The Court of Justice went on to say at [55] that, when choosing the measures to be adopted, the addressee of the injunction had to ensure compliance with the right of internet users to freedom of information. The Court continued:

> "56. In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.

57. It must be possible for national courts to check that that is the case. In the case of an injunction such as that at issue in the main proceedings, the Court notes that, if the internet service provider adopts measures which enable it to achieve the required prohibition, the national courts will not be able to carry out such a review at the stage of the enforcement proceedings if there is no challenge in that regard. Accordingly, in order to prevent the fundamental rights recognised by EU law from precluding the adoption of an injunction such as that at issue in the main proceedings, the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known.

58. As regards intellectual property, it should be pointed out at the outset that it is possible that the enforcement of an injunction such as that in the main proceedings will not lead to a complete cessation of the infringements of the intellectual property right of the persons concerned.

59. First, as has been stated, the addressee of such an injunction has the possibility of avoiding liability, and thus of not adopting some measures that may be achievable, if those measures are not capable of being considered reasonable.

60. Secondly, it is possible that a means of putting a complete end to the infringements of the intellectual property right does not exist or is not in practice achievable, as a result of which some measures taken might be capable of being circumvented in one way or another.

61. The Court notes that there is nothing whatsoever in the wording of Article 17(2) of the Charter to suggest that the right to intellectual property is inviolable and must for that reason be absolutely protected (see, to that effect, *Scarlet Extended*, paragraph 43).

62. None the less, the measures which are taken by the addressee of an injunction, such as that at issue in the main proceedings, when implementing that injunction must be sufficiently effective to ensure genuine protection of the fundamental right at issue, that is to say that they must have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right.

63. Consequently, even though the measures taken when implementing an injunction such as that at issue in the main

> proceedings are not capable of leading, in some circumstances, to a complete cessation of the infringements of the intellectual property right, they cannot however be considered to be incompatible with the requirement that a fair balance be found, in accordance with Article 52(1), in fine, of the Charter, between all applicable fundamental rights, provided that (i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right."

172. Counsel for Richemont submitted that the decision in *Ziggo v BREIN* was wrong, as shown by the subsequent judgment in *UPC v Constantin*. Counsel for the ISPs supported the decision in *Ziggo v BREIN* and submitted that there was nothing inconsistent with it in *UPC v Constantin*.

173. In my judgment it is wrong in principle to interpret Article 3(2) of the Enforcement Directive as requiring rightholders to establish that the relief they seek is likely to reduce the overall level of infringement of their rights. As counsel for Richemont pointed out, Article 3(2) is equally applicable to offline and online infringements. If trade mark owners like Richemont apply for a final injunction to restrain further infringements against a market trader who has been caught selling counterfeit watches, they do not have to show that the injunction is likely to reduce the overall level of infringement of their trade marks. Nor would it be a defence to such an application for the market trader to say "If consumers can't buy counterfeit goods from me, they will simply buy them from other market traders". Nor would the market trader improve his position by pointing to five other traders selling counterfeits in the same market whom the trade mark owner had not yet sued (but intended to sue in due course). To allow such a defence would not only undermine intellectual property rights, it would also be inimical to the rule of law: consider the application of such reasoning to burglars, for example. There is no reason to treat online infringers differently in this respect. Nor is there any reason to treat intermediaries whose services are being used to infringe by third parties differently in this respect.

174. Furthermore, I consider that the judgment of the CJEU in *UPC v Constantin* supports this understanding of the law, for two reasons. First, the Court was explicit at [58]-[61] that it did not matter that the injunction would not lead to a complete cessation of the infringements. Secondly, the Court made it clear at [62] that the measures taken by the addressee of the injunction must at least have the effect of making access to the protected subject-matter difficult to achieve and of seriously discouraging internet users *who are using the services of the addressee* from accessing that subject-matter. The Court did not say that internet users who were using the services of other intermediaries must also be discouraged. Still less did the Court suggest that the addressee would be let off the hook if users used the services of other intermediaries instead.

175. On the other hand, I entirely accept that, as discussed in *20C Fox v BT* at [192] and *EMI v Sky* at [103]-[106], the likely efficacy of the injunction in terms of preventing or impeding access to the target website is an important factor in considering the proportionality of a website blocking injunction. It is evident from the CJEU's judgment in *UPC v Constantin* that the applicable criterion of efficacy is whether the measures required by the injunction will at least seriously discourage users from accessing the target website.

176. Furthermore, despite what I have said above, I also accept that what the ISPs' solicitor Michael Skrein described in his evidence as the "substitutability" of unblocked websites for the blocked one is also a factor to be taken into account in considering proportionality. Although the rightholder does not have to show that blocking access to the target website is likely to reduce the overall level of infringement in order to obtain relief, blocking access to the target website is less likely to be proportionate if there is a large number of alternative websites which are likely to be equally accessible and appealing to the interested user than if that is not the case.

Dissuasive

177. Article 3(2) of the Enforcement Directive requires that remedies for infringement of intellectual property rights be "dissuasive". Although counsel for the ISPs submitted that dissuasiveness was a separate requirement to the other requirements listed in paragraph 158 above, she did not address it separately in her submissions. As I understood it, this was on the footing that it added nothing to the other requirements, and in particular the requirement of effectiveness, in the circumstances of this case.

178. I disagree with this approach. Article 3(2) of the Enforcement Directive requires that remedies for intellectual property infringement shall not merely be effective, but also dissuasive. As I see it, the distinction between the two is that effectiveness relates to the defendant, whereas dissuasiveness relates to third parties. That is to say, the remedies granted against the defendant should dissuade third parties from infringing in the future. This function is particularly reflected in recital (27) and Article 15 of the Directive. It is also recognised by the reasoning of the CJEU in the passage from *UPC v Constantin* quoted in paragraph 171 above.

179. In my judgment, it follows that, when deciding whether or not to grant a website blocking injunction, it is relevant for the court to consider whether it is likely to have such a dissuasive effect.

Not unnecessarily complicated or costly

180. Article 3(1) of the Enforcement Directive requires that remedies "shall not be unnecessarily complicated or costly". Although in context this appears to be a requirement that remedies should not be unnecessarily complicated or costly for the rightholder to obtain, as counsel for the ISPs pointed out, the CJEU has interpreted the requirement as applying more generally. Thus in Case C-70/10 *Scarlet Extended SA Société Belge des Auteurs, Compositeurs et Editeurs Scrl (SABAM)* [2011] ECR I-11959 the Court stated at [48]:

> "Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its

> business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly."

See also Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA v Netlog NV* [2012] 2 CMLR 18 at [46] and *L'Oréal v eBay* at [139].

181. On the other hand, the CJEU has also held in *UPC v Constantin* at [50] that a website blocking injunction is not necessarily objectionable because it obliges the addressee "to take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions". Reading the judgment in *UPC v Constantin* as a whole, I consider that what the CJEU is saying is that the difficulty and cost of complying with the injunction are factors to be taken into account in assessing the proportionality of such an injunction.

Avoidance of barriers to legitimate trade

182. Article 3(2) of the Enforcement Directive requires that remedies "shall be applied in such a manner as to avoid the creation of barriers to legitimate trade". Counsel for the ISPs relied on the manner in which this requirement had been interpreted by the CJEU in *L'Oréal v eBay* at [140], but in the present context I consider that what the CJEU said in *UPC v Constantin* at [56] (quoted in paragraph 171 above) is more pertinent: the measures adopted by the ISP must be strictly targeted so that they do not affect users who are using the ISP's services in order lawfully to access information. If that is done, then not only will the remedy respect the users' rights under Article 11 of the Charter, but also it will not create a barrier to legitimate trade.

Fair and equitable and fair balance

183. Article 3(1) of the Enforcement Directive requires that remedies "shall be fair and equitable". I consider that, at least in the present context, this amounts to the same thing as the requirement that they be proportionate. The same goes for the requirement discussed below for a "fair balance" to be struck between the various fundamental rights which are engaged.

Proportionate

184. As I noted in *Golden Eye (International) Ltd v Telefónica UK Ltd* [2012] EWHC 723 (Ch), [2012] RPC 28 at [116], there are two reasons why it is necessary to consider the proportionality of orders in this field. The first is that Article 3(2) of the Enforcement Directive imposes a general requirement that remedies for the infringement of intellectual property rights be proportionate: see *L'Oréal v eBay* at [139]-[144]. The second is that the CJEU has held that, when adopting measures to protect copyright owners against online infringement, national courts must observe the principle of proportionality and strike a fair balance between the protection of intellectual property rights guaranteed by Article 17(2) of the Charter and the protection of the fundamental rights of individuals who are affected by such

measures, and in particular the rights safeguarded by the other applicable Articles of the Charter: see Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271 at [61]-[68], *Scarlet v SABAM* at [42]-[46], [50]-[53], *SABAM v Netlog* at [41]-[51] and *UPC v Constantin* at [46].

185. The principle of proportionality is a general principle of EU law which, as the CJEU stated for example in Case C-2/10 *Azienda Agro-Zootecnica Franchini Sarl v Regione Puglia* [2011] at [73],

> "… requires that measures adopted by Member States in this field do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; where there is a choice between several appropriate measures recourse must be had to the least onerous and the disadvantages caused must not be disproportionate to the aims pursued."

186. The approach to considering proportionality which I set out in *Golden Eye* at [117] was as follows:

> "… First, the Claimants' copyrights are property rights protected by Article 1 of the First Protocol to the ECHR and intellectual property rights within Article 17(2) of the Charter. Secondly, the right to privacy under Article 8(1) ECHR/Article 7 of the Charter and the right to the protection of personal data under Article 8 of the Charter are engaged by the present claim. Thirdly, the Claimants' copyrights are 'rights of others' within Article 8(2) ECHR/Article 52(1) of the Charter. Fourthly, the approach laid down by Lord Steyn where both Article 8 and Article 10 ECHR rights are involved in *Re S* [2004] UKHL 47, [2005] 1 AC 593 at [17] is also applicable where a balance falls to be struck between Article 1 of the First Protocol/Article 17(2) of the Charter on the one hand and Article 8 ECHR/Article 7 of the Charter and Article 8 of the Charter on the other hand. That approach is as follows: (i) neither Article as such has precedence over the other; (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' - must be applied to each."

187. This statement of the law was approved by Lord Kerr of Tonaghmore JSC delivering the judgment of the Supreme Court in *Rugby Football Union v Viagogo Ltd* [2012] UKSC 55, [2012] 1 WLR 3333 at [45].

188. In the present case, Richemont rely on trade marks, which are also intellectual property rights within Article 17(2) of the Charter. The other rights which are engaged by the orders sought by Richemont are (i) the ISPs' freedom to conduct business

under Article 16 of the Charter and (ii) the freedom of information of internet users under Article 11 of the Charter: see *UPC v Constantin* at [47].

189. For the reasons discussed above, I conclude that, in considering the proportionality of the orders sought by Richemont, the following considerations are particularly important:

i) The comparative importance of the rights that are engaged and the justifications for interfering with those rights.

ii) The availability of alternative measures which are less onerous.

iii) The efficacy of the measures which the orders require to be adopted by the ISPs, and in particular whether they will seriously discourage the ISPs' subscribers from accessing the Target Websites.

iv) The costs associated with those measures, and in particular the costs of implementing the measures.

v) The dissuasiveness of those measures.

vi) The impact of those measures on lawful users of the internet.

190. In addition, it is relevant to consider the substitutability of other websites for the Target Websites.

Safeguards against abuse

191. In addition to the requirements listed by counsel for the ISPs, the solicitor for the ORG pointed out that Article 3(2) of the Enforcement Directive requires remedies to be applied in such a manner as to "provide for safeguards against their abuse". I entirely accept this. I shall consider what it entails below.

Application to the present case

192. Applying these principles to the present case, my assessment is as follows.

The comparative importance of the rights engaged and the justifications for interfering with those rights

193. In the present context, this requires the Court to consider the comparative importance of, and the justifications for interfering with, Richemont's trade mark rights on the one hand and the ISPs' freedom to carry on business and internet users' freedom to receive information on the other hand.

194. So far as Richemont's trade mark rights are concerned, for the reasons given above, it is clear that the Target Websites are infringing the Trade Marks by advertising, offering for sale and selling counterfeit goods. Richemont have a legitimate interest in curtailing such activity, because it is damaging to Richemont in the ways described in paragraph 14 above. There is also a public interest in preventing trade mark infringement, particularly where counterfeit goods are involved.

195. As to the ISPs' freedom to carry on business, the orders sought by Richemont would not impair the substance of this right. The orders would not interfere with the provision by the ISPs of their services to their customers. The orders would not require the ISPs to acquire new technology: they have the requisite technology already. Indeed, most of the ISPs now have greater technical capacity to implement such orders than they did three years ago. The main effect of the orders would be to impose additional operating costs on the ISPs. It is true that there is a small risk of the ISPs being attacked either by hackers or by operators of the Target Websites, but in my judgment this risk is not a significant one. It is also true that there is a risk of reputational damage to the ISPs, particularly in the event of overblocking, but again I do not consider this risk a significant one.

196. As for the freedom of internet users to receive information, this plainly does not extend to a right to engage in trade mark infringement, particularly where it involves counterfeit goods. Since the Target Websites appear to be exclusively engaged in infringing commercial activity, with no lawful component to their businesses, the operators have no right which requires protection. Thus the key consideration so far as this freedom is concerned is the impact of the orders on users of other, lawful websites. If the orders are properly targeted, and have sufficient safeguards built into them, then that should mean that such users are not affected.

Availability of alternative measures

197. The ISPs' arguments and evidence in the present case focussed heavily on the availability of alternative measures. It is common ground that there are a variety of measures which Richemont could adopt to try and combat the infringements of the Trade Marks by the Target Websites. The dispute is as to the comparative efficacy and burden of the alternative measures.

198. *Action against the operators*. The first step which Richemont could take, and have taken, is to send cease and desist letters to the named registrants of the domain names as identified by a WHOIS search. Unsurprisingly, these letters were simply ignored. Since the registrants all gave addresses outside the United Kingdom, many in China, Richemont faced obvious difficulties of jurisdiction and/or enforcement if they were to attempt to bring proceedings against the registrants. Furthermore, the registrants may not be the actual operators of the Target Websites. Experience in the copyright context shows that it is frequently difficult to identify the real operators of offending websites and that attempts to bring proceedings against the operators are rarely effective. Accordingly, I do not consider that this is a realistic alternative measure.

199. *Notice and takedown by hosts.* The second step which Richemont could take, but have not taken, is to send notices to the hosts of the Target Websites demanding that the Target Websites be taken down. It is common ground that, in principle, the most effective means of removing offending websites from the internet is takedown by the host. It is also common ground that, where a website is hosted by a reputable host in countries such as EU Member States, the USA and so on, it is usually possible for intellectual property owners to get infringing websites taken down. This is because such hosts have usage policies which prohibit (among other things) intellectual property infringement and contractual terms which permit takedown in the event of breach of those policies. Usually, it is not necessary for the rightholder to obtain a court order against the host to enforce such terms.

200. As the ISPs pointed out, the Target Websites all appear to be hosted by reputable hosts which are mostly based in the USA or an EU Member State (although one is based in Malaysia). The hosts could be quickly, easily and inexpensively contacted by email or telephone to notify them of the infringements and request that the Target Websites be taken down. Although Richemont queried whether such requests would be complied with, on the evidence presently before the court I consider that it is probable that they would be complied with by most of the current hosts.

201. More importantly, Richemont contend that notice and takedown is ineffective because, as soon as an offending website is taken down by one host, the almost invariable response of the operator is to move the website to a different host. Furthermore, the likelihood is that, sooner or later, the website will be moved to a host, typically based offshore or in a non-Western jurisdiction, which does not respond to notice and takedown requests. Still further, once that happens, the intellectual property owner faces obvious difficulties in jurisdiction and/or enforcement if it attempts to bring proceedings against the host to compel it to take down the website. I accept that experience in the copyright context bears out Richemont's contentions in this regard. Accordingly, I consider that, while Richemont are open to criticism for not even having attempted to use this measure, it is unlikely that it would be effective to achieve anything other than short-term disruption of the Target Websites.

202. This leads to what I consider to be one of the central debates on the present application. Counsel for the ISPs submitted that notice-and-takedown was a less burdensome measure than website blocking both for Richemont and for the ISPs. Counsel for Richemont submitted that it was more burdensome for Richemont. He argued that one of the key advantages of website blocking from the rightholders' perspective was that the updating machinery built into the orders provided a mechanism for dealing with circumvention by the website operators which was not only more effective in the long run than notice-and-takedown, but also less burdensome. In particular, he argued that it was less burdensome because it enabled the rightholders to use automated procedures such as Incopro's BlockWatch to update the orders and hence the blocking carried out by the ISPs. He did not dispute that notice-and-takedown was less burdensome for the ISPs, but he submitted that there was scope for the ISPs to deal with updating requests more efficiently than they currently did.

203. Dealing with the latter point first, the ISPs' riposte was to dispute that they were inefficient and to say that the rightholders should provide update requests in a more consistent and efficient manner. I would encourage the two sides to have constructive discussions over ways in which the process can be streamlined so as to make it more efficient for both. Nevertheless, it is obvious that website blocking orders impose compliance costs on the ISPs, whereas notice-and-takedown requests to the hosts do not.

204. Turning to the position of the rightholders, I accept that website blocking has advantages over notice-and-takedown. Accordingly, I am not persuaded that, overall, notice-and-takedown is an equally effective, but less onerous, measure. The key question, to my mind, is whether the benefits of website blocking, which accrue to the rightholders, justify the costs, and in particular the implementation costs which are imposed on the ISPs. This question is central to the assessment of proportionality.

205. *Payment freezing*. A third measure which Richemont could adopt, but have not adopted, is to ask the payment processors used by the Target Websites, such as Visa, MasterCard and Western Union, to suspend the operators' merchant accounts. These payment providers have contractual terms which enable them to suspend a merchant's account where the merchant has been involved in supplying counterfeit goods. This has the advantage that the effect is felt worldwide and not merely in the UK. It is not clear from the evidence to what extent this can be achieved without a court order, however.

206. Richemont's evidence is that there are two problems with this approach. The first is that, although it may diminish the circulation of counterfeit goods, it leaves the offending website untouched. Thus at least the first category of infringement will continue until such time as the website is so starved of funds that it ceases operation, assuming that that time does come. The second is that, as with notice-and-takedown, the websites simply shift to alternative payment methods. Indeed, there is evidence that in some cases such websites display the logos of processors such as Visa to give the appearance of legitimacy, but do not actually accept payment by that means. The customer only discovers this after he or she has placed an order and is asked to pay by an alternative method. The cartierloveonline website provides an example of this (see paragraph 22 above). Furthermore, a number of the Target Websites state that they accept payment by bank transfer, among other methods.

207. My conclusion in relation to this measure is similar to my conclusion in relation to notice-and-takedown. While Richemont are open to criticism for not even having attempted to contact the payment processors, it is unlikely that this would be effective to achieve more than some degree of disruption to the Target Websites. Again, therefore, I do not regard the availability of this alternative measure as a complete answer to Richemont's application, but it falls to be taken into account in the proportionality analysis.

208. *Domain name seizure*. A fourth measure which Richemont could adopt, but have not adopted, is to seize the domain names of the Target Websites by invoking the dispute resolution procedures ("DRPs") of the registrar through which the domain names have been purchased on the ground that the domain names include the Trade Marks. This is a more complicated and costly procedure from Richemont's perspective than any of the three measures considered above, but the ISPs point out that a DRP claim would be less costly than the present claim. Again, however, the problem is that the website operator can simply pick a new domain name and start again. Accordingly, I am not persuaded that this is a realistic alternative measure in general, although there may be particular cases where it has some value.

209. A variation of this measure is for Richemont to attempt to persuade a law enforcement agency, such as the Police Intellectual Property Crime Unit ("PIPCU"), to take action to have the domain name suspended or cancelled. This is only possible in the case of UK domains, however. In any event, the essential problem remains the same. This is illustrated by what happened in the case of one of the Target Websites. On 1 May 2014 the domain name ukmontblancoutlet.co.uk was suspended as a result of action by PIPCU, but the very next day the Target Website re-appeared under the name montblancoutletonline.co.uk.

210. *De-indexing*. A fifth measure which the ISPs contend that Richemont could adopt, but have not adopted, is to send notices to search engine providers such as Google requesting them to "de-index" the Target Websites. This would have the effect of removing the website from the search engine's search results, thereby preventing consumers from finding the site by that means.

211. In my view this is potentially an important weapon in the armoury of a trade mark owner like Richemont. The reason for this is that it seems reasonably clear that the way in which many consumers find websites like the Target Websites is by searches using search engines. For example, the consumer may search for "replica Cartier watches" or "replica Montblanc pens". If the search engine provider de-indexes a website, then that website will not appear in the search results from such a search.

212. Richemont's evidence, however, is that there are three problems with this approach. The first is that search engine providers are not willing to de-index entire websites on the basis of alleged intellectual property infringements without a court order. Furthermore, although it is clear from the decision of the CJEU in Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos* [EU:C:2014:317], [2014] 3 WLR 658 that search engine providers can be ordered to de-index webpages on privacy grounds, it is not clear at present that any EU court would have power to order de-indexing on the basis of intellectual property infringement.

213. The second problem is that, whereas some search engine providers like Google have adopted a policy under which they are prepared to de-index links to specific URLs which infringe third party copyrights without court orders, they do not have an equivalent policy for URLs which infringe third party trade marks.

214. The third problem is that, even if search engine providers de-index the URL or even the entire website, it will remain accessible on the internet. In particular, it would remain accessible to consumers who had previously visited the website and either had it bookmarked or could remember its domain name. It would also remain accessible to new consumers who were sent the link either in spam emails or via social networks.

215. Accordingly, I conclude that, as matters stand, this is not a realistic alternative measure for Richemont.

216. *Customs seizure*. A final measure is that of customs seizure. This is in fact a measure which Richemont do employ. There are two obvious problems with it, however. The first is that it only tackles the imports of the counterfeit goods themselves. It does not affect the Target Websites. The second is that it is impossible for customs to inspect anything more than a small fraction of the large volume of small parcels that enter the country each day. The proof of the pudding is in the eating: all of the packages the subject of the test purchases from the Target Websites got through without being intercepted by customs.

217. *Conclusion*. For the reasons given above, I am not persuaded that there are alternative measures open to Richemont which would be equally effective, but less burdensome, with the consequence that Richemont's application should be refused on that ground alone. Nevertheless, I do accept that the availability of some of the measures discussed above is a factor to be taken into account in assessing the proportionality of the orders sought by Richemont.

Efficacy

218. For the reasons given above, although I do not accept that it is incumbent on Richemont to show that the blocking measures would lead to a reduction in the overall level of infringement of the Trade Marks, I do accept that the effectiveness of the blocking measures in reducing access to the Target Websites is an important factor in assessing their proportionality.

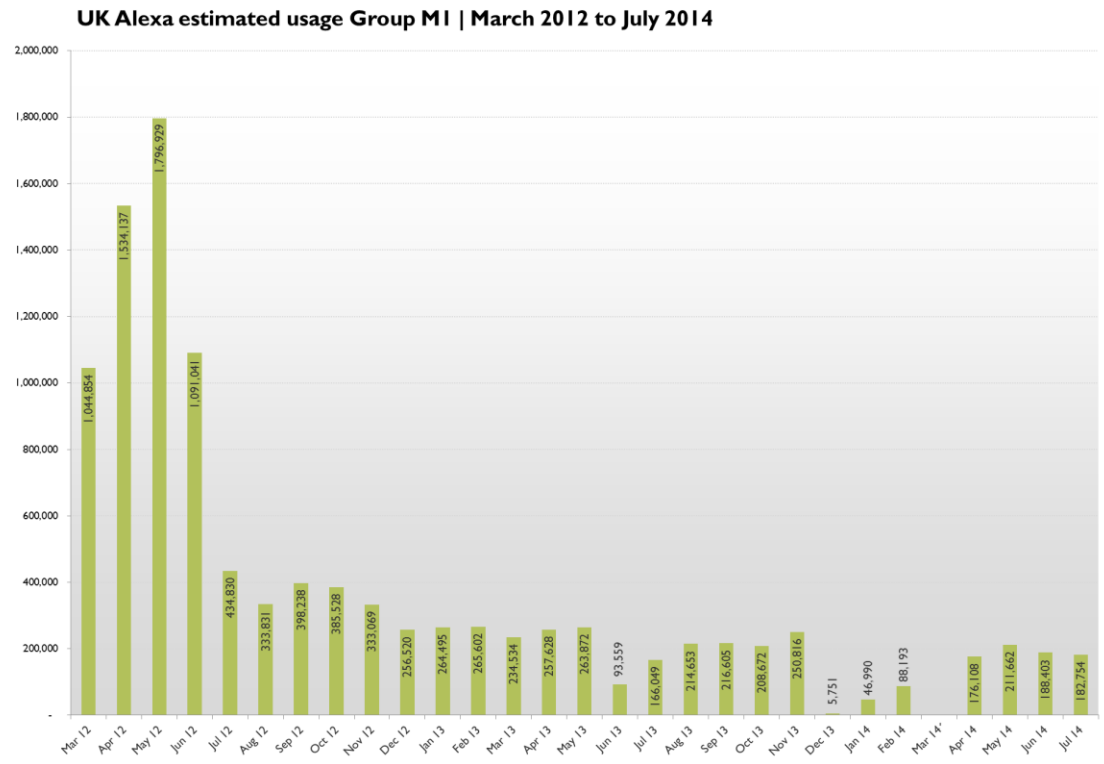
219. There are two aspects to this part of the case. The first aspect concerns the section 97A orders. At the time of *20C Fox v BT*, there was little evidence available as to the efficacy of such measures. Three years later, there is rather more evidence upon which to base an assessment. The second aspect concerns the orders sought in the present case. Even if the evidence shows that the section 97A orders have some degree of effectiveness in reducing access to the websites targeted by those orders, does it follow that the orders sought in the present case would be as effective? I shall deal with these aspects in turn.

220. *The section 97A orders*. As indicated above, evidence as to the efficacy of the section 97A orders has been given by both Ms Saunders and Prof Brown. Ms Saunders analysed the efficacy of the order using data collected by Incopro's Site Intelligence Database. The data in question is internet traffic data provided by Alexa. Alexa's traffic data is extrapolated from sample data from millions of internet users who form Alexa's global traffic panel. Incopro collects various different types of Alexa data for websites on its database. For present purposes, Incopro calculates an "Alexa estimated usage" metric from the Alexa global three month reach data, which is expressed as the number of users per million, by multiplying it by the number of internet users. Where there is enough traffic available, Alexa makes data available for individual countries and Incopro can calculate the estimated usage for those countries.

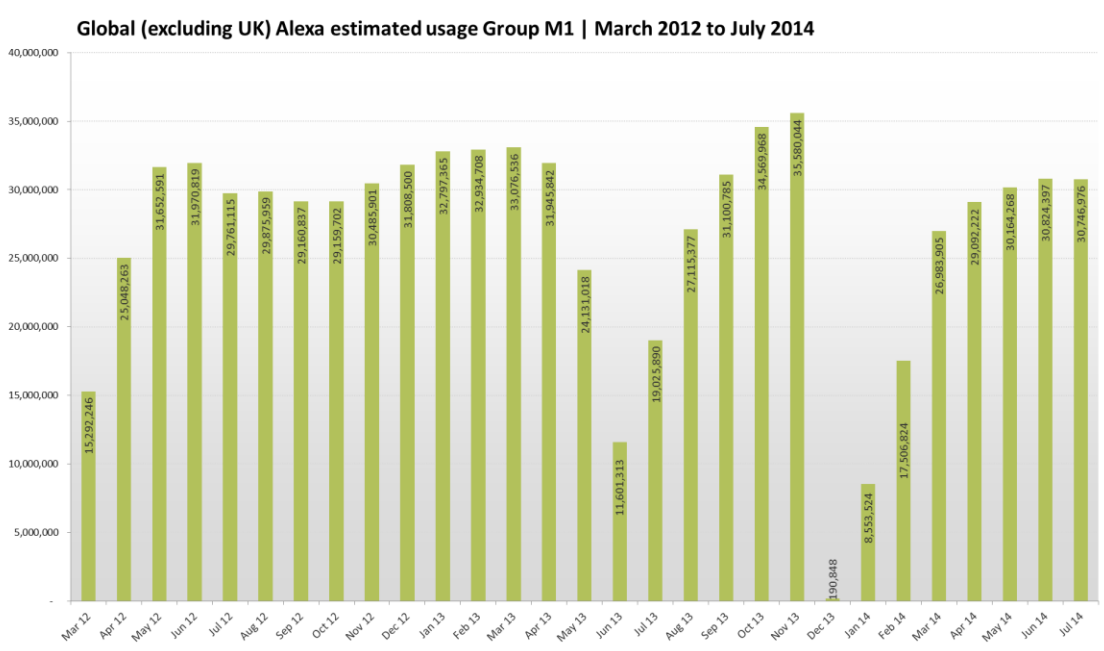
221. Ms Saunders has analysed the Alexa estimated usage data for the UK in respect of each of the websites targeted by the section 97A orders, in most cases from January 2013 to July 2014. There are two exceptions to this. First, in the case of TPB, she has analysed data from March 2012 to July 2014. Secondly, in the case of Newzbin2 and FirstRow, she has not been able to carry out an analysis because of insufficient data. Ms Saunders has carried out comparative analyses of the Alexa estimated usage data for the world excluding the UK.

222. Ms Saunders' analyses show a consistent pattern. In each case, the UK data show a marked and sustained drop in traffic to the targeted websites after the date on which the blocking order was implemented. By comparison, the global data excluding the UK do not show anything like this. By way of illustration, I shall take the data for TPB. This is admittedly one of the more dramatic examples in Ms Saunders' report, but I have chosen this example for reasons that will appear.

223. The following graph shows the UK Alexa estimated usage from March 2013 to July 2014 for TPB's primary domain.



224. The following graph shows the global (excluding the UK) Alexa estimated usage for the same group of sites.

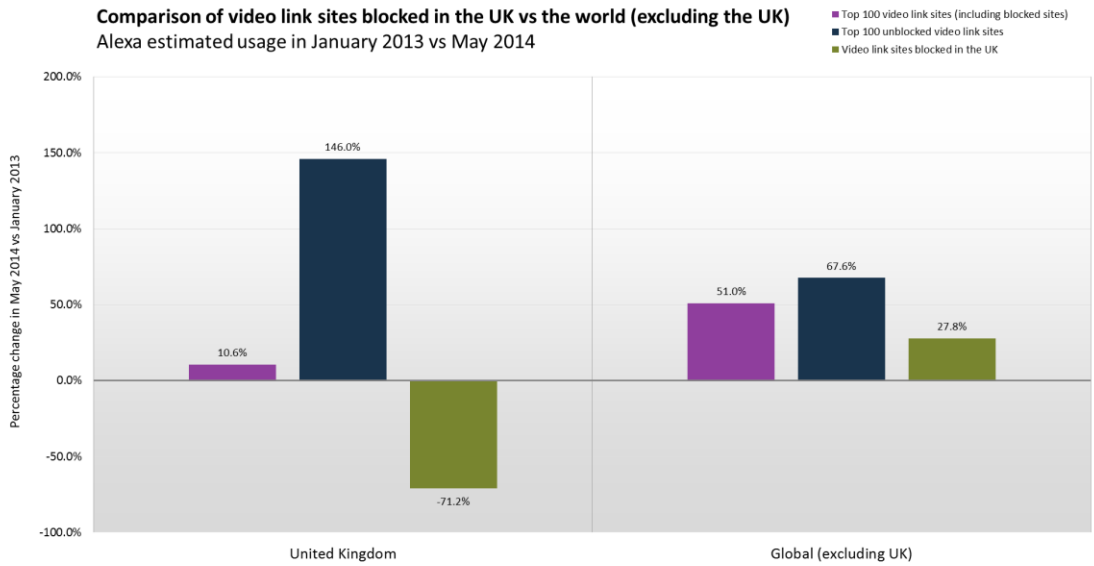


225. Ms Saunders explains that the dips in usage observed in the second graph coincided with TPB changing domain names. Overall, it can be seen that there is a striking contrast between the UK traffic and the global traffic.

226. In addition to the analyses described above, Ms Saunders also analysed Alexa estimated usage data for proxies, concluding that there was no evidence of any major migration of UK users of the targeted websites to proxies. She also analysed data for

searches for search terms relating to VPNs and Tor using Google Trends. This data shows a steady increase in such searches since 2007, but no correlation with the dates of implementation of any of the section 97A orders.

227. Finally, Ms Saunders compared the Alexa usage data for the top 100 video streaming link websites (i.e. websites which infringe film and television copyrights) in the Incopro database in the UK with the global data excluding the UK for the period January 2013 to May 2014. The resulting graph is reproduced below (UK on the left, rest of the world on the right).



228. This graph is particularly interesting. Consistently with the individual analyses of targeted websites discussed above, it shows that the UK has experienced a significant decrease in traffic to blocked websites (-71.2%), whereas the rest of the world has experienced an increase in traffic to those websites (27.8%). On the other hand, the UK has experienced a greater increase in traffic to non-blocked websites (146%) than the rest of the world (67.6%). This suggests that many UK users who have been blocked from accessing websites as a result of section 97A orders have not circumvented the blocks, but have started using different websites instead. Nevertheless, the overall increase in use of these websites is lower for the UK (10.6%) than for the rest of the world (51%). This suggests that the section 97A orders have resulted in a decrease in the overall level of infringement in this sector in the UK.

229. Turning to Prof Brown's report, apart from describing the relative ease with which circumvention may be achieved, he relied upon by the study by Poort *et al* which was cited by the Court of Appeal of The Hague in *Ziggo v BREIN* (see paragraph 167 above). As the authors of the study make clear in their introduction, they considered that "the relevant question is not whether blocking access to TPB [by the six Dutch ISPs] decreased the number of visitors to this website, but what the effect is on online infringement as a whole". Apart from reviewing earlier literature, this study had two main components. The first component consisted of two consumer surveys, the first in May 2012 of 2009 respondents and the second in November-December 2012 of 2422

respondents. The second component consisted of analyses of BitTorrent traffic in April 2012, May 2012 and February 2013.

230. The survey respondents were asked about their purchasing, downloading and streaming of music from legal sources and their downloading and streaming of music and other content from illegal sources during the preceding 6 months, between 6 and 12 months previously and more than a year previously. The respondents to the first survey were asked about their expected reaction to the blocking of TPB, while respondents to the second survey were asked about their actual reaction to the blocking. Respondents were also asked which of the six ISPs they subscribed to. The conclusions drawn by the authors from the survey were as follows:

> "Two consecutive consumer surveys provide insight into consumers' reactions to the intervention after three, six and ten months, as well as the reaction they expect shortly before blocking. The intervention can only affect consumers who download or intend to download from illegal sources, 27-28% over the past year. For this segment of the population, it is found that a large majority (70-72%) is non-responsive to blocking access to TPB. This is significantly more than consumers expect prior to the blocking. About half of those who report a response to the intervention state they download less, while a third state they stopped downloading altogether. The rest claim to download more as a result of the intervention.
>
> This would suggest a small negative *blocking effect* of the intervention on the percentage of the population downloading from illegal sources. However, no such effect is found. Instead, the percentage downloading films & series, games and books from illegal sources in the preceding six months increased between May and November/December 2012, while downloading music from illegal sources remained constant. This implies that any behavioural change in response to blocking access to TPB has had no lasting net impact on the overall number of downloaders from illegal sources, as new consumers have started downloading from illegal sources and people learn to circumvent the blocking while new illegal sources may be launched, causing file sharing to increase again (*relapse effect*)."

231. In my judgment the survey component of this study suffers from two significant limitations. First, the precise survey methodology is not described in the paper, and in particular the actual questions asked are not revealed. It is well known that responses to survey questions are influenced by the phrasing of the questions. Secondly, respondents were being asked to report on their own behaviour, and indeed their own behaviour recollected over extended periods of time. The fact that they were being asked to report unlawful behaviour is not necessarily a problem, since one might expect this to lead to consistent under-reporting (although in this context one should not ignore the possibility that some segments of the population may over-report such activity). The problem is that consumers are not good at accurately recalling and reporting their own behaviour in quantitative terms. A familiar example is that of diet.

The self-reporting by consumers of their own diet is notoriously unreliable. Better results are achieved if consumers are asked to keep a food diary.

232. I would also comment that, if the authors' conclusions are correct, the overall ineffectiveness of the blocking in reducing the overall level of infringement was partly due to new users starting to use file-sharing websites for the first time. This suggests that, without the blocking, there would have been an increase in the overall level of infringement.

233. Turning to the traffic analyses, this is said by the authors to involve "an innovative data collection technique that directly monitors BitTorrent participation by monitoring the distribution of peers for a sample of torrent files". In fact, it appears that a different monitoring program of "improved … effectiveness" was used for the monitoring in February 2013 than the one used in April and May 2012. The monitor used in February 2013 "joins the torrent swarm and records activity, it requests a new set of peers from the tracker as often as allowed and records all these IP addresses". During February 2013 the monitor was used to record activity in ten torrent swarms over a two week period. Each peer record contained the IP address, the torrent it was recorded in and the time. Dutch spoken or subtitled torrents were selected, from which Dutch peers were identified. The conclusion drawn by the authors from the monitoring was as follows:

> "BitTorrent monitoring reveals only small changes in the distribution of Dutch peers over the different ISPs over the three measurements, which implies very limited effect of the intervention on BitTorrent file sharing."

234. In my judgment the monitoring component of the study also suffers from a number of limitations. First, only Dutch spoken and subtitled torrents were selected. As is well known, however, English is very widely spoken in the Netherlands. Furthermore, a great deal of file-sharing involves English language music. Secondly, as noted above, the monitoring program was changed for the last measurement, which makes comparisons with the first two difficult. Thirdly, the monitoring did not attempt to measure behaviour over an extended period of time.

235. Finally, even taking the findings and conclusions of the Poort study entirely at face value, they do not show that the blocking of TPB was ineffective in reducing access to that website in the Netherlands. On the contrary, they show that it did have some effect. Nor is it necessarily the case that the findings can be translated to the UK.

236. Overall, the conclusion which I draw from the evidence is that, in the section 97A context, blocking of targeted websites has proved reasonably effective in reducing use of those websites in the UK. No doubt it is the casual, inexperienced or lazy users who stop visiting those websites, whereas the experienced and determined users circumvent the blocking measures; but that does not mean that it is not a worthwhile outcome.

237. *The present case*. Turning to the present case, how effective would the blocking measures sought by Richemont be in reducing use of the Target Websites by consumers in the UK? In my judgment there is no reason to believe that the blocking would be materially less effective in reducing UK traffic to the Target Websites than

the blocking of the websites targeted by the section 97A orders. If anything, it is probable that it will be more effective. This is because the evidence suggests that users have little "brand loyalty" to websites like the Target Websites, whereas websites like TPB do have quite a loyal user base.

Dissuasiveness

238. In my judgment the orders sought by Richemont would have some dissuasive value, since they would not only result in consumers who attempted to access the Target Websites being blocked from doing so (unless they and/or the operators undertook circumvention measures), but also they would be informed of the reason for this.

Costs

239. There are two aspects to the debate about costs. The first concerns the costs regime which the Court should apply if website blocking orders based on trade mark infringement are granted. Both sides realistically took as their starting point the costs regime which this Court has previously adopted in the context of section 97A orders. In summary, the rightholders bear the costs of the application (other than costs occasioned by the ISPs' resistance to an order), while the ISPs bear the costs of implementation. Similarly, the rightholders bear the costs of monitoring the targeted websites after implementation of the order and notifying the ISPs of updates, while the ISPs bear the costs of implementing such updates.

240. So far as this aspect of the matter is concerned, I adhere to the view that, for the reasons I gave in *20C Fox v BT (No 2)* at [53], the rightholders should pay the costs of an unopposed application. I also adhere to the view that, for the reasons I gave in *20C Fox v BT (No 2)* at [32], the ISPs should generally bear the costs of implementation as part of the costs of carrying on business in this sector. Indeed, it seems to me that my reasoning is supported by the subsequent judgment of the CJEU in *UPC v Constantin* at [50]. Nevertheless, as I said in *20C Fox v BT (No 2)* at [33], I do not rule out the possibility of ordering the rightholder to pay some or all of the implementation costs in an appropriate case. Equally, I consider that it makes sense for the rightholders to bear the costs of monitoring and the ISPs to bear the costs of implementation of updates, subject to the same caveat.

241. The second aspect of the debate concerns the consequences, and in particular the consequences for the ISPs in terms of the costs of implementation, of that approach. So far as this aspect of the matter is concerned, the ISPs did not seriously dispute that the cost of implementing a single website blocking order was modest. As I have explained above, the ISPs already have the requisite technology at their disposal. Furthermore, much of the capital investment in that technology has been made for other reasons, in particular to enable the ISPs to implement the IWF blocking regime and/or parental controls. Still further, some of the ISPs' running costs would also be incurred in any event for the same reasons. It can be seen from the figures I have set out in paragraphs 61-65 above that the marginal cost to each ISP of implementing a single further order is relatively small, even once one includes the ongoing cost of keeping it updated.

242. As counsel for the ISPs emphasised, however, that is not the whole story. From the ISPs' perspective, what really matters is not the cost of implementing a single order,

but the cumulative cost of implementing all website blocking orders. Counsel for Richemont submitted that Richemont's application should be judged on its own merits, and hence solely on the basis of the costs consequences to the ISPs of the orders sought by this application. I do not accept that submission, which in my view does not reflect the reality of the situation. The impact of one order cannot be judged in isolation from the impact of other orders that have been or are likely to be granted.

243. In that regard, the ISPs advance two contentions. The first is that the overall costs burden imposed by implementing section 97A orders is already significant and is growing rapidly. The second is that, if the Court opens the door to the grant of website blocking orders on the grounds of trade mark infringement, the overall costs burden will become substantially greater.

244. So far as the first contention is concerned, both sides reminded me of what I had said in *20C Fox v BT* at [189]:

> "… even if the present application is successful, I think it is clear that rightholders will not undertake future applications lightly. On the contrary, I consider it probable that they will concentrate their resources on seeking relief in respect of the more egregious infringers. I therefore do not anticipate a flood of such applications."

Richemont contend that this prediction has been borne out by subsequent events, whereas the ISPs contend that it has been contradicted. On this point I agree with Richemont. Even taking into account the pending applications referred to in paragraphs 69-71 above, I do not consider that there has been a flood of applications over the past three years. It seems to me that the rightholders have indeed concentrated their resources on seeking relief in respect of the more egregious infringers.

245. So far as the second contention is concerned, it is manifest that granting website blocking orders on trade mark grounds in addition to copyright grounds will increase the overall cost burden on the ISPs. The question is the extent of the increase. As was the case at the time of *20C Fox v BT*, this is an exercise in futurology. Richemont contends that it is probable that, as with orders based on copyright grounds, rightholders seeking orders on trade mark grounds will concentrate their resources on seeking relief in respect of the more egregious infringers and there will not be a flood of applications. The ISPs are concerned, however, that there will be a flood of applications.

246. In this connection, counsel for the ISPs made two powerful points. The first concerns the sheer number of websites which infringe trade marks. In the case of Richemont alone, it is Richemont's own evidence that Richemont have identified approximately 239,000 potentially infringing websites of which approximately 46,000 websites have been confirmed as infringing and are waiting for enforcement action. These are huge numbers.

247. The second point concerns the Target Websites. On what basis were the Target Websites selected for the present application, as opposed to the thousands of other websites? Other than a statement that the Target Websites were identified using

Google searches, this question has not been directly answered in Richemont's evidence, even though it was raised by the ISPs' evidence. Nor is it at all easy to discern the basis on which the Target Websites were selected from the evidence that is before the Court. Unlike websites like TPB, none of them appears to be very popular. The most popular is cartierloveonline.com with a global Alexa ranking of 5,575,490. Two others have global rankings of 6,837,762 and 15,003,668, while the remainder have too little global traffic to be ranked. (None of the Target Websites has enough UK traffic for Alexa to calculate a UK ranking.) Nor is there anything about the nature of the infringements being committed by the Target Websites to distinguish them from many other infringing websites.

248. These two points cause me considerable concern. If the orders sought by Richemont on the present application are granted, then there is clearly the potential for Richemont to apply for a large number of similar orders. The same must be true of many other trade mark owners. The only constraints upon the trade mark owners will be the need to gather the requisite evidence, to bear the costs of the application and to bear the ongoing costs of monitoring the situation to provide updates to the ISPs. Those are real constraints, but it is difficult to predict the extent to which trade mark owners will be inhibited by them.

249. Counsel for Richemont submitted that the implementation costs imposed on the ISPs by website blocking orders were very small compared to the ISPs' total operating costs. For example, Sky's operating costs for the year ended 30 June 2013 were in excess of £6 billion, while BT's operating costs for the year ended 31 January 2014 were in excess of £12 billion. Counsel for the ISPs correctly pointed out that these are the total operating costs for the companies' entire businesses, which include other activities in addition to providing access to the internet. The ISPs have not condescended to provide the operating costs of their internet access businesses, however. In those circumstances, I accept that the implementation costs imposed on the ISPs by website blocking orders are presently small compared to the operating costs of the ISPs' internet access businesses. For the reasons I have discussed, however, the implementation costs are likely to increase, and it is difficult to foresee by how much.

250. The ISPs have given evidence as to the likely future implementation costs if a substantial number of orders are granted. I see no reason to think that these are anything other than genuine estimates. Nevertheless, it is manifest that they involve a considerable degree of speculation. For my part, I would be surprised if the costs proved to be as high as envisaged by some of the estimates, at least in the short to medium term.

251. Before expressing a conclusion on the question of costs, it is necessary to consider the economic dimension of the problem. Surprisingly, this was not something that was addressed by either side, whether in argument or evidence. As can be seen from recital (59) to the Information Society Directive, the economic logic of granting injunctions against intermediaries such as ISPs is that they are the "lowest cost avoiders" of infringement. That is to say, it is economically more efficient to require intermediaries to take action to prevent infringement occurring via their services than it is to require rightholders to take action directly against infringers. Whether that is correct as a matter of economics is not for me to judge. Nor is it for me to judge whether it is good policy in other ways. That judgement has already been made by the

legislators when they adopted Article 8(3) of Information Society Directive and Article 11 of the Enforcement Directive, in return for the immunities from infringement claims and the exception from general monitoring granted to ISPs and others under Articles 12-15 of the E-Commerce Directive.

252. The economic question does not end there, however. It is obvious that ISPs faced with the costs of implementing website orders have a choice. They may either absorb these costs themselves, resulting in slightly lower profit margins, or they may pass these costs on to their subscribers in the form of higher subscription charges. Clearly it is important that none of the ISPs should gain a competitive advantage over the others, but this is ensured by the fact that they are all required to take approximately equivalent measures. Given a level playing field, the ISPs may choose to pass these costs on to their subscribers. The effect of this would be the familiar one of requiring the community as a whole (in this case, the community of broadband users in the UK) to pay the costs of law enforcement action against the minority of people who behave unlawfully or who take advantage of the unlawful behaviour of others (in this case, by accessing infringing websites). This is a solution that has been adopted in many other contexts, most obviously in the funding of police forces through general taxation. It follows that the ISPs would not necessarily be the ones who would ultimately bear these costs. (The same applies to the costs of implementing the IWF blocking regime and parental control systems, of course.)

253. My conclusion on the question of costs is that, assuming the same costs regime is applied as in the case of section 97A, the likely cost to the ISPs of implementing website blocking orders is an important factor in assessing the proportionality of the orders sought. I am not persuaded, however, that the implementation costs on their own lead to the conclusion that the orders should be refused.

Impact on lawful users

254. Given that the Target Websites are wholly engaged in infringing activity, the impact of the orders sought by Richemont on lawful users depends on two factors. The first is whether each Target Website shares an IP address with another website, and if so whether that other website carries on a lawful activity. The second is the precise nature of the order which Richemont seek.

255. So far as the first factor is concerned, there is no dispute that five of the six active Target Websites share an IP address with other websites. For example, as at 18 September 2014, cartierloveonline.com shared an IP address with 13 other websites, two of which were cartierlove2u.com and cartierlove2u.net. Richemont's solicitors have analysed the other 11 websites. Their conclusion is that nine of them were advertising counterfeit goods (in two cases replica Cartier goods and in the other cases goods unconnected with Cartier, including Nike and Beats by Dr Dre). One was unavailable and one was a holding page with links to other illegitimate websites. Similar conclusions were reached in respect of four other Target Websites. The details of these analyses were only produced after the hearing, however, and the ISPs' solicitors have indicated that they are not entirely accepted by the ISPs.

256. So far as the second factor is concerned, Richemont contend that, in the case of the Target Website which does not share an IP address, then an order which required IP address blocking would not adversely affect lawful users. I accept this. Richemont

also contend that, in the case of Target Websites which share an IP address with other websites which are engaged in unlawful activity, then an order which required IP address blocking would not adversely affect lawful users of the internet. In principle, I agree with this. Whether the other websites are in fact engaged in unlawful activity depends on the accuracy of Richemont's solicitors' analyses, however. If the ISPs consider that the position is open to doubt, they are entitled to require the Court to decide the question. If necessary, I will hear further argument on this point. Finally, Richemont accept that, if a Target Website shares an IP address with a legitimate website, then the order should only require DNS blocking.

257. In conclusion, it ought to be possible to target the blocking so that lawful users are not adversely affected by it.

Substitutability

258. The ISPs contend that other websites are highly substitutable for the Target Websites. This is for four main reasons, all of which I have already touched on above. First, there are a huge number of other infringing websites. Secondly, there is nothing unique about the Target Websites. Thirdly, the Target Websites are not very popular, and do not have much loyalty amongst their customers. Fourthly, it appears that many consumers find such websites through searches using search engines. I accept that these points indicate that consumers are very likely to turn to other websites if the Target Websites are blocked.

259. Against this, Richemont rely on evidence that blocking a relatively small number of websites would lead to all of the links on the first two pages of search results for a Google search for e.g. "buy Cartier replicas" being "dead" links. I have to say that I am somewhat sceptical about this, since my understanding of the way in which search engines work is that the number of visits websites receive is an important factor in ranking search results and that the ranking is territory-specific.

Overall assessment of proportionality

260. None of the arguments and evidence that I have heard and read in this case have caused me to alter my view as to the proportionality of the section 97A orders which have been granted by this Court. It does not necessarily follow that the orders sought by Richemont are proportionate, however. The Court is being asked to exercise its jurisdiction in a new situation.

261. In my view the key question on proportionality is whether the likely costs burden on the ISPs is justified by the likely efficacy of the blocking measures and the consequent benefit to Richemont having regard to the alternative measures which are available to Richemont and to the substitutability of the Target Websites. Having given this question careful consideration, the conclusion I have reached, after some hesitation, is that it is justified. Accordingly, I consider that the orders are proportionate and strike a fair balance between the respective rights that are engaged, including the rights of individuals who may be affected by the orders but who are not before the Court.

Safeguards against abuse

262. The orders sought by Richemont contain a number of safeguards against abuse, including the following. First, they permit the ISPs to apply to the Court to discharge or vary the orders in the event of any material change of circumstances, including in respect of the costs, consequences for the parties and effectiveness of the blocking measures from time to time. Secondly, they permit the operators of the Target Websites to apply to the Court to discharge or vary the orders.

263. There are three further safeguards which I consider should be included, however. The background to the first two is as follows. As can be seen from my judgment in *20C Fox v BT (No 2)*, I permitted someone who claimed to be a BT user to intervene to make written submissions, although, for the reasons I explained, I gave those submissions limited weight in that particular case. In theory, it would have been open to subscribers to the ISPs to apply to intervene in the present case. I note that in *UPC v Constantin* the CJEU held at [57] that "the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known". As discussed above, that statement was made in the context of considering orders which constituted a general prohibition of outcome. It is debatable whether it is applicable to the present situation, and, if so, whether the theoretical possibility of intervening before the order is made complies with this requirement. It is also debatable whether, under English procedural law, users affected by an order once made would be able to apply to discharge or vary it in the absence of an express permission to apply. In order to make sure that the rights of users are protected, I consider that in future orders should expressly permit affected subscribers to apply to the Court to discharge or vary the orders.

264. This leads to the second safeguard. The ORG suggested that the page displayed to users who attempt to access blocked websites should contain further information than is currently the case. I agree with this, up to a point. In my view the page should not merely state that access to the website has been blocked by court order, but also should identify the party or parties which obtained the order and state that affected users have the right to apply to the Court to discharge or vary the order.

265. The third safeguard arises out of another suggestion made by the ORG, namely that website blocking orders should not endure longer than necessary. The section 97A orders made by this Court have all been open-ended, because it has not been possible to predict how long the orders may need to endure. Instead, they have, as discussed above, made provision for them to be discharged or varied in the event of a change of circumstances. In the present case, however, I am concerned about the number of websites that Richemont and other trade mark owners may seek to target and the substitutability of such websites. In view of these concerns, I have concluded that I should incorporate a "sunset clause" into the orders, such that the orders will cease to have effect at the end of a defined period unless either the ISPs consent to the orders being continued or the Court orders that they should be continued. This will enable the practical operation of the orders to be reviewed in the light of experience. I will hear argument as to the appropriate period, but my provisional view is that it should be two years.

Conclusion

266. For the reasons given above, I will make orders substantially in the form sought by Richemont, subject to the two modifications to which I have just referred. I will hear counsel on the precise wording of the orders, as well as any other matters arising.