



Neutral Citation Number: [2019] EWHC 2376 (Ch)

Case No: IL-2019-000078

**IN THE HIGH COURT OF JUSTICE**  
**BUSINESS AND PROPERTY COURTS**  
**INTELLECTUAL PROPERTY LIST (CHANCERY DIVISION)**

Rolls Building  
Fetter Lane, London, EC4A 1NL

Date: 10 September 2019

Before :

**MR JUSTICE ARNOLD**

Between :

**NINTENDO CO., LTD**

- and -

**(1) SKY UK LIMITED**

**(2) BRITISH TELECOMMUNICATIONS PLC**

**(3) EE LIMITED**

**(4) TALKTALK TELECOM LIMITED**

**(5) VIRGIN MEDIA LIMITED**

**Claimant**

**Defendants**

**Benet Brandreth QC** (instructed by **Mishcon de Reya LLP**) filed written submissions on behalf of the **Claimant**

The **Defendants** were not represented

The application was considered on paper

**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.

.....  
MR JUSTICE ARNOLD

## MR JUSTICE ARNOLD :

### Introduction

1. By this claim the Claimant (“NCL”) seeks an injunction requiring the Defendants, who are the five main retail internet service providers (“ISPs”) in the United Kingdom, to take measures to block, or at least impede, access by their customers to four websites (“the Target Websites”) which advertise, distribute, offer for sale and/or sell devices that allow technological protection measures (“TPMs”) on NCL’s popular Nintendo Switch games console to be circumvented. Two of the Target Websites (“the Team Xecuter Websites”) are operated by the parties responsible for developing the circumvention devices. The third and fourth (“the R4 Website” and the “Stargate Website”) are operated by UK resellers of the circumvention devices. All four Websites use NCL’s trade marks.
2. In so far as it relies on the protection of trade mark rights as its basis, the present application is straightforwardly based on the principles set out by the Court of Appeal in *Cartier International AG v British Sky Broadcasting Ltd* [2016] EWCA Civ 658, [2016] ETMR 43 and refined by the Supreme Court in the same case [2018] UKSC 28, [2018] 1 WLR 3259. The application raises one novel point, however, in that NCL relies, in addition to its trade mark rights, on the statutory protection given by sections 296ZD and 296 of the Copyright, Designs and Patents Act 1988 (“CDPA88”) against the circumvention of copyright protection measures. NCL accepts that the rights conferred by sections 296ZD and 296 CDPA88 are not themselves intellectual property rights and therefore fall outside the ambit of European Parliament and Council Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (“the Enforcement Directive”), but contends that the reasoning of the Supreme Court in *Cartier* demonstrates that this is no obstacle to the present application.
3. The First Defendant consents to the application, while the other Defendants do not oppose it. As I have observed on previous applications for blocking injunctions, however, that does not absolve the Court from its responsibility to ensure that the application is well founded before granting it.

### NCL and its intellectual property rights

4. NCL is a well-known Japanese company that designs, manufactures and sells video games consoles, accessories and software. One of its most successful products to date is a console called the Nintendo Switch. NCL has sold millions of Nintendo Switch consoles in the UK. Games for the Nintendo Switch are written both by NCL and by third parties referred to as “Authorised Developers” who operate under a programme which NCL says is cheap to join, user-friendly and benefits from extensive support from NCL. Out of the 2100 games currently available for the Nintendo Switch, 1804 were developed by Authorised Developers.
5. NCL is the proprietor of various relevant intellectual property rights. Both the Nintendo Switch and the games include copyright works such as the operating software (referred to as “firmware”) embedded in the Nintendo Switch, the software for the games that run on the Nintendo Switch and various other copyright works such

as the sound-track, graphics, text and so forth that are included in the operating environment and games.

6. NCL is also the proprietor of various trade marks. For present purposes, two EU Trade Marks are relied upon (“the Trade Marks”), both of which are registered for “programs for consumer video games, memory cards storing programs for consumer video game apparatus; storage media storing programs for consumer video game apparatus; programs for handheld electronic game apparatus” in class 9 and “consumer video game apparatus; parts and accessories for consumer video game apparatus” in class 28:
  - i) EUTM No. 16070914 for the word mark NINTENDO SWITCH, which was registered on 4 May 2017.
  - ii) EUTM No. 016606873 for the figurative mark depicted below (referred to as “the Joycon logo”), which registered on 18 September 2017:



#### The TPMs

7. The TPMs employ symmetric and asymmetric encryption to protect the copyright works. In simplified outline, an authorised video game is encrypted using a unique key. Attempts to decrypt the game without the correct key will produce unintelligible results. When an authorised user purchases a game, they are supplied with the encrypted game and with a unique key known as the title key, itself encrypted using a common key, and further encrypted using a device key unique to the individual console. The title key may then be decrypted by the authorised user first using the device key then the common key, the decrypted title key is then deployed to decrypt the game itself. As well as encryption of the game software, encryption is used to create a digital signature that ensures that the source of the software being supplied is authorised. The operation of the TPMs relies on the presence of various encryption keys in the firmware in the Nintendo Switch.
8. Regrettably, third parties discovered that there was a way to circumvent the TPMs by installing custom firmware on the Nintendo Switch. NCL implemented a change to the Nintendo Switch to prevent this in June 2018, but there remains a very substantial number of the earlier, vulnerable Nintendo Switch consoles in circulation and there is evidence of active attempts being made to circumvent the TPMs even on the post-June 2018 Nintendo Switches.

#### The circumvention devices

9. The circumvention devices consist of the SX Pro, which comprises a USB dongle and a jig tool, together with software called SX OS. Having purchased an SX Pro from a reseller, the user downloads SX OS from the first of the Target Websites onto a blank

microSD card which the user inserts into his or her Nintendo Switch together with the SX Pro. The user then goes to the second of the Target Websites and, using a licence key stored in the SX Pro, obtains a licence for SX OS, which is then operable on the user's Nintendo Switch.

### The Target Websites

10. Copies of screenshots of the Target Websites are annexed to the Particulars of Claim. For present purposes, the following features are pertinent.

11. The first Target Website, which is located at the URL team-xecuter.com, is shown at pages 12-34 in Annex 2:

- i) In a green bar at the top of the home page shown on page 12 are hyperlinks in yellow that link to various other parts of the website and, in the case of that entitled "SX Family Portal", link to the second Target Website discussed below.
- ii) In the middle of the home page there is a headline "SX OS v2.8 Beta Announcement" below which is a picture of the screen of a Nintendo Switch with SX OS installed on it. The central icon of three icons displayed on the screen is NCL's Joycon logo.
- iii) On the left-hand side is a box headed "where to purchase" that has the SX logo on the left and proclaims on the right: "If you are looking to buy our SX Family of Team Xecuter products, then please check out our Where To Buy page, listing all of our many valued local and worldwide resellers, as below is just a short recommended list by us."
- iv) Below this on the left-hand side there are adverts for resellers in various countries such as Canada, and (on page 13) France, Germany, and Spain.
- v) Turning to page 18, at the bottom of the page just above the video box, in a section headed "SX OS v2.7 Beta Announcement", there is a statement "Of course, behind the scenes we are also still working hard on our solution for those 'unhackable' switches. Good progress is being made, so hang in there!".
- vi) Page 24 shows the "About Us" page. On the left is a PayPal Instant Delivery advert that offers "USA/EU shipping". The About Us section explains:

"Team Xecuter have developed hardware and software for the Xbox Scene since 2001. The initial roots of the group were based on the Xbox homebrew hacking scene, however where we started as a small group of hardcore enthusiasts dealing with extremely gray area market products, we have now grown into a large electrical manufacturer that develops products for many companies around the world.

Our heart still lies within the games console community and we are always active in developing new and innovative products that we ourselves use in our gaming lives. Whereas we have

long digressed from trading in areas that have now been made illegal in most countries over the years, our ambition is to continue to product quality items at an affordable price.”

- vii) Page 27 show the “Where to Buy” page. This explains, in the middle of the page, that “On this page you will find a updated list of all our authorized resellers around the world that have available our latest Xecuter SX Family Products”. Below that is listed a reseller that is said to offer “Shipping worldwide”.
  - viii) Starting at page 29 is a “List of Resellers operating within Europe (choose the one best for your area for shipping rates).”
  - ix) On page 30, beside an Irish flag, are listings for “Stores Based in Ireland” that includes, as the first listed, the fourth Target Website (Stargate).
  - x) On page 32, beside a Union flag, is a list of “Stores based in the United Kingdom”. The second link down is to the third Target Website (R4).
12. The second Target Website, located at the URL [sx.xecuter.com](http://sx.xecuter.com), is shown at pages 35 to 41 of Annex 2. This Target Website is accessed by clicking on the hyperlink on the first Target Website entitled “SX Family Portal”. It is at the second Target Website that a user obtains a license for the SX OS. The link to do this is at the top right of page 35 labelled “Activate SX OS”. It is also possible to download updated versions of the SX OS, as can be seen from page 36. NCL contends, and I accept, that it can be seen that, in this and other ways, the two Team Xecuter Websites operate in conjunction with each other. In addition:
- i) On page 35 there is statement “Introducing SX by Team Xecuter The ultimate solution for **jailbreaking** your Nintendo Switch has arrived”.
  - ii) Turning to page 37, in the middle of the page there is a heading SX OS, below which it is explained that “SX OS is our revolutionary Custom Firmware for Nintendo Switch”. In the images below this is shown, as the top picture, the screen of a Nintendo Switch onto which SX OS has been installed, with, in the central picture, the Joycon logo displayed. Around the images are various pieces of information about SX OS. At top left it is explained that it works “with every Nintendo Switch console **released before June 2018**”. On the left at the bottom of the page it is explained that you can “Play All Games!”
  - iii) On page 38, under heading “Homebrew Games & Apps” it is stated that “Using SX OS homebrew menu launcher you can enjoy all the quality games and software by independent developers”.
  - iv) On pages 40-41 are instructions for the use of SX Pro and SX OS. Installing the SX OS promises, as stage 5, that the user can “Enjoy the latest games and homebrew!”.
13. The third Target Website (R4), currently located at the URL [sxflashcart.com](http://sxflashcart.com), is shown at Annex 3:

- i) At page 43, in the top right, below the box marked “Cart”, there is a hyperlink labelled “HACK AMIIBO/SWITCH”. In the second row of “new arrivals” on the left there is advertised the “Switch Xecuter SX OS” and “Switch Xecuter SX Pro and OS”.
  - ii) On page 44 in the top left there are two more adverts for the circumvention devices. The second of these shows a Nintendo Switch on which can be seen the screen with SX OS loaded and, in the centre, the Joycon logo. The prices are all in sterling.
  - iii) On page 45, middle right, is a section entitled “Hack your Switch 3DS New 2DS by a flashcart.” Below the title it states “Flashcard is the best choice to play free games in UK Ireland”. The fourth line states “To hack Nintendo Switch, just buy the Xecuter SX Pro and OS”. In the bottom right, under “Store Information” it states “SX Flashcart UK”.
  - iv) On page 46 is the page reached by clicking the hyperlink “HACK AMIIBO/SWITCH” referred to in the opening sub-paragraph above. In the title box it states “...We support all kinds of Nintendo Switch accessories to play Nintendo Switch games.” Below that are further adverts for the circumvention devices including the image of the Nintendo Switch with the custom firmware installed on which the Joycon logo appears.
  - v) On page 47 are various adverts for the circumvention devices. Among them, on the left-hand column and accompanied by an image of the Nintendo Switch, is an offer for “Switch Xecuter SX Pro and OS” with the words “The Nintendo Switch has been hacked already by Xecuter SX Pro and OS” appearing beneath.
  - vi) On page 50 is the page reached by clicking the hyperlink for one of the adverts for “Switch Xecuter SX Pro and OS”. The blurb beneath the title states “The Nintendo Switch has been hacked... with this Switch flashcart Xecuter SX the players can enjoy free custom firmware without limits... It can support all the regions....” Similar information is given under the heading “More Info” at the bottom of the page.
  - vii) On page 51 further information about the product is provided. The second bullet point under “Why buy Switch Xecuter SX?” explains “An original Switch cartridge is too expensive, we can save our money to enjoy free games.” At the bottom of the page are customer reviews, two of which are from “Ryan P”: the top one states “...I ordered from the UK and item was here in 6 days with free shipping method....” The second one states “... I used free postage option to the UK, it took about 8 days to arrive...”
  - viii) On page 52 the second review from the bottom from “Ash B” states “arrived in the UK 05/06/2018”.
14. The fourth Target Website (Stargate), currently located at the URL [xecuteros.com](http://xecuteros.com) but previously located at [stargate3ds.org](http://stargate3ds.org), is shown at Annex 4:

- i) At page 60 is the home page. The website is entitled “Stargate3DS” and next to the title is a “.UK” logo. In the middle of the page there are three purchase options for the circumvention devices, all priced in sterling. The image of the left-hand option shows the Nintendo Switch with SX OS installed and displaying a screen that has on it the Joycon logo.
- ii) On page 61 in the right-hand column are brief explanations of the Switch Xecuter SX OS “...software to hack Nintendo Switch console...” and the Switch Team Xecuter SX Pro and OS modchip which “hacks Nintendo Switch”.
- iii) On page 63 at the bottom right is “Store Information”, which gives an address in “Staybridge UK”.
- iv) At page 65 is the page one reaches by clicking on the option to buy the Switch Xecuter SX OS. The description of the product states “The Switch Xecuter SX OS is a software to hack Nintendo Switch console. It’s easy and cheap to pirate a Switch. With Switch Xecuter SX OS, the players can play all kinds of Switch games freely.”
- v) On page 66 the “characteristics” of the product are said to include “Compatible with games outside the regions”. Below that is a section headed “Why buy Xecuter SX OS in stargate3ds.org?” The third bullet point promises “All orders in stargate3ds.org are sent free with the tracking number and arrived quickly in UK!”
- vi) At page 68 is shown the page one reaches by clicking on the option to buy the Switch Team Xecuter SX Pro and OS modchip. The description includes information similar to that shown on page 65 but also states in the final sentence “To pre order a Switch SX flashcart to begin your hack journey in UK and Ireland”. At the bottom of the page under “More Info” it explains “The main function of Switch Xecuter SX flashcart is to install CFW [Custom FirmWare] on your Nintendo Switch consoles. After the custom firmware setup on the console you can start to play downloaded free Nintendo Switch games so that we don’t need to buy expensive retail cartridge from amazon or ebay.”

#### UK access and test purchases

15. NCL’s evidence shows that persons located in the UK have been able to access the Target Websites using the Defendants’ services. In addition, a person located in the UK was able to purchase a Switch Xecuter SX Pro and OS from the R4 Website and a Switch Xecuter SX Pro and SX OS modchip from the Stargate Website, both of which were delivered to the UK. Using the device purchased from the R4 Website it was possible to install SX OS on a Nintendo Switch and then download and run unauthorised games. Similarly, the device purchased from Stargate could be installed on a Nintendo Switch.

Trade mark infringement

16. NCL's primary case of trade infringement is the operators of the Target Websites are infringing the Trade Marks under Article 9(2)(a) of European Parliament and Council Regulation 2017/1001/EU of 14 June 2017 on the EU trade mark ("the EU Trade Mark Regulation"). In my judgment it is beyond dispute that each of the Target Websites are using signs identical to the Trade Marks in the course of trade in relation to goods identical to those for which the Trade Marks are registered without NCL's consent. That leaves three questions to be considered, First, is the use liable to affect one of the functions of the Trade Marks? Secondly, do the Target Websites target consumers in the UK? Thirdly, do the operators of the Target Websites have a defence under Article 14(c)?
17. So far as the first question is concerned, NCL contends that the answer is yes for three reasons. First, even if the majority of consumers are not confused as to the origin of the goods, the presentation of the Target Websites will lead a significant number of consumers wrongly to believe that these are authorised accessories. That is sufficient for a finding of infringement: see in particular *Interflora Inc v Marks & Spencer plc* [2014] EWCA Civ 1403, [2015] BusLR 492 at [107]-[130].
18. Secondly, there is the prospect of post-sale confusion where, for example, a Nintendo Switch on which the software has been loaded is viewed by third parties and the Joycon logo that appears on the loading screen of SX OS is seen: see in particular Case C-206/01 *Arsenal Football Club plc v Reed* [2002] ECR I-10273.
19. Thirdly, even if there is no effect on the origin identification function, there is an effect on the other functions and in particular the investment function: see in particular Case C-323/09 *Interflora Inc v Marks & Spencer plc* [2011] ECR I-8625 at [62]-[63]. The use of NCL's Marks by the Target Websites is expressly intended to undermine the integrity of NCL's console and game software and as such "interferes with the proprietor's use of its trade mark to acquire or preserve a reputation capable of attracting consumers and retaining their loyalty."
20. In my judgment each of these contentions is well founded. In relation to the first contention, it seems to me that the majority of consumers would appreciate from all the references to "hacking" that the Target Websites were offering unauthorised products designed to enable circumvention of TPMs, but I consider that the presentation of the websites, and in particular statements such as the "About Us" statement quoted in sub-paragraph 11(vi) above, which give the impression that the Team Executor websites are legitimate, is likely to deceive a significant number of consumers.
21. NCL's secondary case is that the operators of the Target Websites have infringed the Trade Marks pursuant to Article 9(2)(c). NCL contends that the Trade Marks benefit from a very substantial reputation as a result of the use made of them and that the use by the Target Websites without due cause takes unfair advantage of the reputation of the Trade Marks by intentionally exploiting that reputation in order to sell the circumvention devices. Again, I accept this.
22. Turning to the question of targeting, the relevant principles were considered by the Court of Appeal in *Merck KgaA v Merck Sharpe & Dohme* [2017] EWCA Civ 1834,



[2018] ETMR 10 at [153]-[170]. In my judgment the presentation of each of the Target Websites shows that they target consumers in the UK. While the second Target Website on its own might not do so, it operates in conjunction with the first Target Websites which does. Moreover, the test purchases clearly establish that the R4 and Stargate Websites target UK consumers and use of the devices sold by those Websites requires use of the second Target Website.

23. As to whether there could be defence under Article 14(c), NCL contends that this does not apply for two reasons. First, because a significant number of consumers would be misled: see in particular *Bayerische Motoren Werke AG v Technosport London Ltd* [2017] EWCA Civ 779, [2017] FSR 35 at [18]. Secondly, because the operators' use is not in accordance with honest practices in industrial and commercial matters since the purpose of the circumvention devices is to allow users to circumvent the TPMs and to play unauthorised games. I accept these contentions.

### Circumvention of the TPMs

24. As noted above, NCL also relies on the provisions of sections 296ZD and 296CDPA88, which respectively implement Article 6 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") and Article 7(1)(c) of European Parliament and Council Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs ("the Software Directive").
25. Section 296ZD addresses the protection of copyright works other than computer programs and provides (in relevant part):

"(1) This section applies where—

- (a) effective technological measures have been applied to a copyright work other than a computer program; and
- (b) a person (C) manufactures, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire, or has in his possession for commercial purposes any device, product or component, or provides services which—
  - (i) are promoted, advertised or marketed for the purpose of the circumvention of, or
  - (ii) have only a limited commercially significant purpose or use other than to circumvent, or
  - (iii) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, those measures.

- (2) The following persons have the same rights against C as a copyright owner has in respect of an infringement of copyright—
- (a) a person—
    - (i) issuing to the public copies of, or
    - (ii) communicating to the public,  
the work to which effective technological measures have been applied;
  - (b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a); and
  - (c) the owner or exclusive licensee of any intellectual property right in the effective technological measures applied to the work.”
26. The interpretation of this provision and its application has been considered in a number of cases. A helpful review of the issues that arise was given by Floyd J (as he then was) in *Nintendo Company Ltd v Playables Ltd* [2010] EWHC 1932 (Ch), [2010] FSR 36. Since then, the Court of Justice of the European Union has considered Article 6 of the Information Society Directive in Case C-355/12 *Nintendo Co Ltd v PC Box Srl* [EU:C:2014:25].
27. The CJEU explained at [27] that Article 6 is to be interpreted broadly and “includes application of an access control or protection process, such as encryption, scrambling or other transformation of the work”. NCL contends, and I accept, that this covers the TPMs in this case, which encrypt the video games including their artwork, text, and soundtracks to prevent unauthorised copies being created or played on the Nintendo Switch console. It is no objection that these copyright works are supplied as part of the software: see *Playables* at [25].
28. The CJEU went on at [31] to hold that the measures must be proportionate to the aim of protecting copyright, being “suitable to achieve that objective and must not go beyond what is necessary for this purpose”. In making that assessment the CJEU pointed, at [33], to the relative costs of different types of technological measure, consideration of technical and practical aspects of their implementation, and comparison of the effectiveness of different types of technological measures. NCL’s evidence is that these TPMs represent good practice and that alternative measures would increase costs to consumers. In making the assessment, it is also relevant to consider the actual use of the circumvention devices: see *PC Box* at [36]. Although it might be said that the circumvention devices can be used to play “homebrew” games on the Switch, it is clear that they are used primarily to play pirated games. That is how they are promoted – as allowing the playing of “free” games. Accordingly, the circumvention devices are directed towards enabling circumvention of the TPMs so as to enable unlawful use of the Nintendo Switch. Nor does the presence of the TPMs inhibit independent development of video games for the Nintendo Switch since NCL

provides an easy route to doing so via its Authorised Developer program. Accordingly, I am satisfied that the TPMs are proportionate.

29. The next issue that arises is whether the operators of the Target Websites fall within sub-section (1)(b). It is plain from review of the Target Websites that they do on any of the bases set out in sub-sections (i) to (iii). As noted above, the circumvention devices are expressly stated to be for “hacking” the Nintendo Switch.
30. The next question is whether NCL has standing to sue under sub-section (2)(a), (b) or (c). NCL qualifies under each of the potential sub-sections: it is the copyright owner in both the works and the TPMs as well as the party that issues the video games to the public through its eShop.
31. Finally, NCL accepts that, as with its claim for infringement of the Trade Marks, the activities complained of must be targeted at the UK since the rights conferred by section 296ZD are designed to protect UK copyrights. I have already considered this issue and the answer is the same in this context.
32. Section 296 CDPA88 applies to protection of computer programs. It provides (in relevant part) as follows:
  - “(1) This section applies where--
    - (a) a technical device has been applied to a computer program; and
    - (b) a person (A) knowing or having reason to believe that it will be used to make infringing copies--
      - (i) manufactures for sale or hire, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire or has in his possession for commercial purposes any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of the technical device; or
      - (ii) publishes information intended to enable or assist persons to remove or circumvent the technical device.
  - (2) The following persons have the same rights against A as a copyright owner has in respect of an infringement of copyright--
    - (a) a person--
      - (i) issuing to the public copies of, or
      - (ii) communicating to the public,

the computer program to which the technical device has been applied;

- (b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a);
  - (c) the owner or exclusive licensee of any intellectual property right in the technical device applied to the computer program.”
33. The application of this section was again considered in *Playables*. Floyd J doubted whether the knowledge requirement in sub-section (1)(b) correctly implemented the Software Directive because there was no such knowledge requirement there, but because *Playables* was an application for summary judgment proceeded on the basis that it did. NCL invites the court to adopt the same approach here. It contends that the requirement for knowledge that the circumvention devices will be used to make infringing copies is clearly met since each of the Target Websites makes a point of the fact that what is being offered is a circumvention device that allows use to download and use infringing copies of relevant works: see for example the statement on the Stargate Website “It’s easy and cheap to pirate a Switch. With Switch Xecuter SX OS, the players can play all kinds of Switch games freely.” I accept this.
34. The other requirements of the section are similar to those in section 296ZD. Although this section refers to “a technical device” rather than to “effective technological measures” the meaning of the term is wide and encompasses the encryption applied to NCL’s software: see *Playables* at [33]. It is clear from review of the Target Websites that they knowingly offer for commercial purposes circumvention devices whose express sole purpose is to circumvent the TPMs. NCL has standing to sue on all three of the sub-sections 2(a), (b) and (c). The activities complained of are targeted at the UK.
35. Accordingly, I conclude that NCL has good claims against the operators of the Target Websites under sections 296ZD and 296 CDPA88 as well as for infringement of the Trade Marks.

#### Jurisdiction to grant a website-blocking injunction

36. The Court’s jurisdiction to grant website-blocking injunctions in cases involving infringement of intellectual property rights notwithstanding the absence of any legislative implementation by the United Kingdom of the third sentence of Article 11 of the Enforcement Directive is now established at the highest level by the decision of the Supreme Court in *Cartier*. As NCL points out, however, it is clear from the reasoning of Lord Sumption (with whom the other members of the Court agreed) at [15] that the Court’s jurisdiction is not limited to cases involving infringement of IP rights:

“Website blocking orders clearly require more than the mere disclosure of information. But I think that it is clear from the authorities and correct in principle that orders for the disclosure of information are only one, admittedly common, category of order which a court may make against a third party to prevent the use of his facilities to commit or facilitate a wrong. I therefore agree with the view expressed by Briggs LJ in his dissenting judgment in the Court of Appeal that the website blocking order made in this case could have been made quite

apart from the power derived from European law, on ordinary principles of equity.”

37. NCL contends, and I accept, that it follows that the Court has jurisdiction to grant NCL the order it seeks not only on the basis of its claims for infringement of the Trade Marks, but also on the basis of its claims for infringement of its rights under sections 296ZD and 296 CDPA88.

Threshold conditions

38. The Court of Appeal in *Cartier* confirmed at [80]-[81] that, in intellectual property cases, there are four threshold conditions which need to be satisfied in order for a website-blocking injunction to be granted:
- i) the defendants are intermediaries within the meaning of Article 11 of the Enforcement Directive,
  - ii) the users and/or operators of the website are infringing the claimants’ IP rights,
  - iii) those users and/or operators are using the defendants’ services to infringe; and
  - iv) the defendants have actual knowledge of this (which may be as a result of being notified by the rightholder).
39. Counsel for NCL submits that analogous criteria should be applied in cases which are not based on infringement of IP rights. I agree with this subject to the qualification that it may not be necessary for the defendants to be intermediaries within the meaning of Article 11 of the Enforcement Directive (although in website-blocking cases defendants usually are). In the case of the fourth criterion, as counsel rightly points out, this follows from the provisions 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”), which is a horizontal measure that is not restricted to cases involving IP rights.
40. Turning to the question of whether the threshold criteria are satisfied in the present case, NCL contends and I accept that:
- i) it is well established that the Defendants are intermediaries;
  - ii) for the reasons given above, the operators of the Target Websites are infringing NCL’s rights in the UK;
  - iii) the evidence establishes that the operators are using the Defendants’ services to do this; and
  - iv) the Defendants have actual knowledge of this, because they have been notified by NCL.

Should an injunction be granted?

41. The Court of Appeal in *Cartier* confirmed at [100]-[128] that, in intellectual property cases, in deciding whether to grant a website-blocking injunction the Court must consider eight criteria over and above the threshold conditions. The injunction must be (i) necessary, (ii) effective, (iii) dissuasive, (iv) not unduly costly or complicated, (v) avoid barriers to legitimate trade, (vi) a fair balance between the fundamental rights engaged, (vii) proportionate and (viii) safeguarded against abuse. Of these factors, proportionality is the key one, since consideration of the other factors feeds into the proportionality analysis.
42. Counsel for NCL submits that the same factors should be considered in a case based on other kinds of rights. I agree with this. Although the criteria set out above are largely drawn from the Enforcement Directive, it can be seen from the jurisprudence of the Court of Justice of the European Union that they largely reflect general principles of EU law, and to some extent principles of European human rights law. Moreover, there is no reason of principle why an application based on other kinds of rights should be subject to either more or less stringent criteria.
43. NCL contends, and I accept, that in the present case these criteria are satisfied because, in summary:
  - i) The injunction sought is necessary to prevent, or at least reduce, substantial damage to NCL. It appears that substantial sales of the circumvention devices have been made in the UK, that substantial quantities of pirated games have been downloaded in the UK and installed on Nintendo Switches using the circumvention devices and that NCL has sustained significant losses as a result. No alternative measures are realistically available to NCL since NCL has been unable to identify the operators of the Target Websites, who may well be abroad. Cease and desist letters sent by NCL's solicitors have been ignored, except that both the R4 and Stargates Websites changed their URLs following the sending of the letters. Take-down requests to the relevant hosting providers, to the extent that these can be identified, have likewise been ignored. Take-down requests sent by NCL to platforms such as YouTube, Amazon and ebay are actioned by the platforms, but the relevant listings are simply replaced by new ones.
  - ii) The evidence in the *Cartier* case showed that, although quite easily circumvented, blocking injunctions are effective in reducing traffic to the target websites.
  - iii) Similarly, blocking injunctions are dissuasive. Moreover, the Defendants are required to display information about the block, which helps to dissuade users.
  - iv) Blocking injunctions are not difficult for the Defendants to implement. On the contrary, they already have the necessary technology. Moreover, as a result of the decision of the Supreme Court in *Cartier*, NCL must bear the Defendants' incremental costs of implementing the injunction, and so there is no additional cost for the Defendants.

- v) The injunction sought by NCL will have no impact on legitimate trade, because none of the Target Websites appears to carry on any legitimate trade.
- vi) The injunction strikes a fair balance between protecting NCL's rights and the rights engaged, because the Defendants' right to carry on business is unaffected and the public has no legitimate interest in being informed about or purchasing circumvention devices whose sole purpose is to circumvent NCL's TPMs and infringe its rights to NCL's significant detriment.
- vii) For the reasons given above, the injunction is proportionate.
- viii) The order proposed by NCL contains the usual safeguards adopted in previous cases.

Conclusion

44. For the reasons given above, I will grant NCL the order it seeks.