Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 753-778

This document is part of the Comparative Study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member states, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

UNITED KINGDOM

1. Legal Sources

The blocking, filtering and take-down of illegal internet content in the UK is **not governed by legislation specific to the internet**. Instead, it predominantly derives from **private regulation** either through the application of *terms of use* policies of internet service providers ("ISPs"), **voluntary cooperation by ISPs** with police, copyright owners and other authorities, or **partnerships between ISPs** and domain name hosts and privately-run industry regulatory bodies.

Acts of Parliament and secondary legislation which address, on a general basis, copyright, defamation and terrorist activities, do contain **some provisions specific to the removal of online material by ISPs**. In England and Wales, the **High Court is empowered to issue orders**, on a case by case basis, against ISPs to block or takedown online content which is defamatory or which infringes copyright. More recently, in the absence of specific legislation, a general power of the High Court to issue injunctions, "*in all cases where it appears to be just and convenient to do so*," was relied on to block web addresses which breached trademark rights. The High Court similarly relies on **general statutory provisions** in the fields of **privacy law and data protection** to issue injunctions which may include a direct or indirect requirement on an ISP to remove or block particular online material.

Other provisions in terrorism legislation and a recently introduced Defamation Act afford exemption from liability to ISPs which act in accordance with **notice and take-down rules**.

Many international standards contained in conventions relating to illegal internet content have **not been transposed** into the domestic regulatory framework. The Council of Europe's ***Convention on Cybercrime*** **was ratified by the UK** in May 2011, although most of its requirements were already fulfilled by the UK Government through a variety of existing domestic legislative provisions,[1] including its procedural requirements, which had already been met by the UK in the form of statutory mutual assistance provisions.[2] **Other Council of Europe Conventions**, such as the *Additional Protocol to the Convention on Cybercrime*, the *Convention on Prevention of Terrorism* and the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* have **not yet been ratified** by the UK Government, although the latter two have been signed. The ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** was however ratified by the UK in 1987 and provisions of the EU's Data Protection Directive 95/46/EC were **transposed into UK law by the Data Protection Act 1998**.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

The legal framework governing the blocking and/or filtering of illegal internet content in the UK is characterized by Internet Service Provider ("ISP") **self-regulation.** As it is not possible for individuals to access the internet without using the services of an ISP, ISPs are said to act as internet information gatekeepers. Accordingly, they are tasked with ever-increasing regulatory responsibilities.[3] This approach is supplemented by **legislation in limited areas,** and **court orders** in the form of injunctions.

---

1 Such as the Police and Justice Act 2006.

2 Contained in the Crime (International Cooperation) Act 2003.

3 See A. Murray, *Information Technology Law*, 2nd ed., Oxford, 2013, p. 71.

The mass blocking and filtering of websites by ISPs in the UK is principally concerned with those which contain **child abuse material** and the **encouragement of terrorism**. Both this, and systems for combatting **domain name abuse** and **internet piracy**, in practice, operate on a voluntary basis through collaboration by ISPs with the UK police, the internet registry, and other private regulators. It might be said that the relative effectiveness of this approach has largely had the effect of diminishing political pressure to legislate further in this area.[4] Where the need arises, rights holders have increasingly been able to benefit from **injunctions** issued by the High Court, on a case-by-case basis, against ISPs. Such injunctions require them to block access to websites found to infringe **copyright or trademarks**. In the fields of **defamation** and **privacy** law, injunctions may also be issued in certain circumstances, which directly or indirectly require ISPs who provide access to websites containing the offending material, to prevent access.

2.1.1. Blocking/filtering of child abuse and obscene adult content

The most high-profile role for ISPs is their collective involvement in preventing access to **child abuse images** and other illegal content. This is achieved by a partnership between the ISPs and an industry regulatory body known as the **Internet Watch Foundation ("IWF")**. The IWF's remit, it says, is to minimize the availability of potentially criminal internet content,[5] specifically: (a) child sexual abuse content hosted anywhere in the world; (b) criminally obscene adult content hosted in the UK, and; (c) non-photographic child sexual abuse images hosted in the UK.[6]

The IWF itself has existed in some form since 1996 and is not a government body or law enforcement agency, but instead, a registered charity, funded by the European Union and the wider online industry. It has no special legal right to intentionally view child sexual abuse material, but relies on protection afforded by a **memorandum of understanding** between the Association of Chief Police Officers ("ACPO") and the Crown Prosecution Service ("CPS"), as part of which the CPS agree not to prosecute professionals involved in the discovery or reporting of indecent images of children in electronic communications media.[7] The IWF also draws its legitimacy from member trade associations and associated internal codes of conduct. The UK **Internet Service Providers Association ("ISPA")**, the UK's trade association for ISPs, defers to the IWF with regard to filtering the unlawful content.[8] Members are bound by **ISPA's Code of Practice**,[9] which states that membership in the IWF

---

4 See *ibid,* where, with reference to the implementation by ISPs of a blacklist of child abuse websites, the author states: "*Failure to implement a private regulatory system would have led to legislation compelling ISPs to filter access.*" As will be seen, the UK Government has also refrained from introducing measures to implement legislation designed to tackle online piracy, in favour of a voluntary industry agreement.

5 Note that this does not include peer-to-peer file sharing activities.

6 Internet Watch Foundation web site, *Remit, Vision and Mission*, available at https://www.iwf.org.uk/about-iwf/remit-vision-and-mission (24.03.2015). For more information on the process of removal and blocking, see section 3.1. of this country report, below.

7 See Open Rights Group web pages, *Internet Watch Foundation*, available at https://wiki.openrightsgroup.org/wiki/Internet_Watch_Foundation (24.03.2015). Memorandum of Understanding available at https://www.iwf.org.uk/assets/media/hotline/SOA2003_mou_final_oct_2004.pdf (24.03.2015). The Sexual Offences Act 2003 also includes a defence (at section 46) to a charge of "making" such images (under the Protection of Children Act 1978) where they can prove that it was necessary for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings.

8 E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation*, International Journal of Law and Information Technology, 2012, Vol. 20 No. 4, p. 317

9 Internet Service Providers Association, *Code of Practice*, available at http://www.ispa.org.uk/about-us/ispa-code-of-practice/ (24.03.2015).

is not mandatory, but that ISPA co-operates with the IWF and that its procedures in this regard are mandatory for ISPA members.

The IWF facilitates the blocking of content by creating a blacklist of sites which contain child sexual abuse images and videos hosted abroad.[10] This blacklist, known as the **Child Abuse Image Content list**, is distributed to all UK ISPs, who may then block access to all sites contained on the list. The IWF says that although it compiles and provides the list of child sexual abuse URLs, the blocking or filtering solution is entirely a matter for the company deploying it.[11] In 2014, a total 28,226 unique *URLs* were included on the list at some point, and the list contained an average of 791 *URLs* per day.[12] The IWF publishes a document entitled, "*URL List Policies, Procedures and Processes*"[13] which consolidates the various procedures and policies relating to the *URL* list, as well as ***Blocking Good Practice*** guidance on its website designed to, "*maintain the principle of transparency and minimise over-blocking and latency issues.*"[14]

It is understood that the **Terms of Service and Acceptable Use Policies of leading ISPs refer to and defer to the IWF** by agreeing to block access to those web pages identified by the IWF. The IWF reports that more than 98% of residential broadband connections are protected by ISPs deploying the list.[15] Although the blocking of such websites is not required by law, the legitimisation by the ISPA and its acceptance by ISPs themselves means the IWF is, in effect, the industry's standard setting body for the filtering of child abuse material.[16]

In the absence of legal safeguards against over-blocking, the IWF has taken a number of steps to better ensure that its operations in this regard are transparent and proportionate. For example, it emphasises that the IWF blacklist is targeted at the most specific level (*URLs*) and that it is dynamic, being updated twice daily with URLs added and removed.[17] Moreover, since 2014, new recommended splash page text for companies which implement the blacklist has been available for them to display on the pages of *URLs* they have blocked. This provides details about why the page is blocked and where users who seek access to the page can go for personal help, as well as how they may use the IWF's *Content Assessment Appeal Process*.[18] The Appeal Process itself offers the possibility for any party with a legitimate association with the content or a potential victim, hosting company, publisher or internet consumer who believes they are being prevented from accessing

---

10 Content hosted in the UK is not added to the URL blacklist, as in such cases, removal at source via notice and takedown procedures are used (see section 2.2.1. of this country report, below). The illegality of the material is determined in line with relevant criminal legislation relating to indecent photographs of children as defined by the Protection of Children Act 1978 and the Sexual Offences Act 2003, extreme pornography as defined by sections 63 – 67 of the Criminal Justice and Immigration Act 2008 and prohibited images of children defined by section 62 of the Coroners and Justice Act 2009. See IWF, *Laws Relating to the IWF's Remit* for further details, available at https://www.iwf.org.uk/hotline/the-laws (24.03.2015).

11 Internet Watch Foundation, *IWF Annual Report 2014*, p.15, available at https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf (10.11.2015)

12 *Ibid.*

13 IWF, *URL List Policies, Procedures and Processes,* available at https://www.iwf.org.uk/assets/media/members/URL%20List%20policies%20procedures%20and%20processes%20FINAL%202.pdf (24.03.2015).

14 IWF, *Blocking Good Practice*, available at https://www.iwf.org.uk/members/member-policies/url-list/blocking-good-practice (24.03.2015).

15 *Ibid.*

16 See E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation*, *op. cit.,* p. 318.

17 See IWF *Annual Report 2014*, *op. cit.*, p. 15.

18 For Splash page wording, see IWF website, *Blocking: Good Practice*, *op. cit.*

legal content to appeal against the accuracy of an assessment.[19] The IWF's Annual Report of 2014 states that in the preceding year, no verified complaints were received from content owners who were concerned that legitimate content which they owned or were associated with had been included on the IWF blacklist.[20]

2.1.2. Blocking/filtering of material encouraging terrorism

Section 3 of the **Terrorism Act 2006**[21] provides the police with the power to require the removal from public availability of **content on the internet deemed to be encouraging or inciting terrorists**. The Counter Terrorism Internet Referral Unit ("CTIRU"),[22] set up by the Home Office[23] and the Association of Chief Police Officers in 2010, is responsible for the co-ordination of take-down notices. It is reported, however, that all removal of unlawful terrorist content is achieved through informal contact between the police and ISPs and that it has never been necessary to use formal powers under the Terrorism Act 2006.[24] The CTIRU also compiles a **blacklist of *URL*s for material hosted outside of the UK** which would give rise to criminal liability under the provisions of the Terrorism Act 2006. These sites are blocked on networks of the public estate, such as government buildings, schools and libraries, meaning that users can still access these websites on private networks. In November 2014, it was announced that **all major UK ISPs would be incorporating the blacklist into their adult content filters**, preventing access to such websites where subscribers do not specifically opt out of such filtering.[25]

There are **no known equivalent legislative provisions in criminal law** by which material amounting to a potential criminal offence may be required to be blocked or filtered. However, it is reported that many ISPs simply remove, on request, material that is illegal or where it breaches their wider terms and conditions of acceptable use.[26]

2.1.3. Domain name abuse

Domain names used for criminal activity, such as **websites offering for sale counterfeit (physical) goods**, those committing fraud ("***phishing sites***") and other **trading standards offences** are effectively blocked by being removed from the internet by *Nominet*, the registry operator for "*.uk*" domain names. By registering a domain name ending in ".uk", the website enters into a contract of

---

19 See section 3.1. of this country report, below, for more detail.

20 IWF, *Annual Report 2014*, *op. cit.*, p. 15.

21 Terrorism Act 2006, available at http://www.legislation.gov.uk/ukpga/2006/11/contents (25.03.2015).

22 ACPO web page, *CTIRU*, available at http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx (25.03.2015).

23 The UK Government department for the interior.

24 House of Lords question to Government, Response of Lord Taylor of Holbeach, Hansard citation: House of Lords Debate, 23 September 2013, c421, available at They Work For You website, http://www.theyworkforyou.com/wrans/?id=2013-09-23a.421.3 (25.03.2015).

25 The Guardian online, news article available at http://www.theguardian.com/technology/2014/nov/14/uk-isps-to-introduce-jihadi-and-terror-content-reporting-button (25.03.2015).

26 See section 2.2.3. of this country report below, and, for example, HM Government, *Challenge it, Report it, Stop it – Delivering the Government's hate crime action plan*, May 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307624/HateCrimeActionPlanProgressReport.pdf (26.03.2015), p. 7.

registration with *Nominet*, fundamental terms of which are that the party in question is entitled to register the domain name and that the domain name will not be used for any unlawful purpose.[27]

Nominet, which describes itself as a private public purpose company, took down more than 2,600 domain names used for criminal activity between December 2009 and March 2011[28] following requests, primarily from public bodies such as the Metropolitan Police E-crime Unit and the Serious Organised Crime Agency.

Action against **websites which commit or support intellectual property crime** through piracy and counterfeiting has also increased in recent years with the launch, in 2013, of the **Police Intellectual Property Crime Unit ("PIPCU")**,[29] a national police unit based in the City of London Police force and funded by the Intellectual Property Office.[30] PIPCU has developed an initiative known as *Operation Creative* under which rights holders identify and report copyright infringing websites to PIPCU. Following assessment by PIPCU officers to verify whether copyright is being infringed, website owners may be contacted by officers to be given the chance to correct their behaviour, and subsequently, the foreign domain name registrar may be contacted to seek suspension of the site. **Ultimately, the website may be placed on an *Infringing Website List* ("IWL")** in order that advertisers, agencies and other intermediaries can voluntarily decide whether to cease advert placement on such sites with a view to disrupting advertising revenues.[31]

Although the **process of putting a website on to the IWL list takes place in the absence of a court order**, it is reported by PIPCU that this will only occur where it is a website determined as being, "*substantially or wholly engaged in copyright crime*," [32] and where efforts to engage with the website owner and the domain name registrar have not been successful.[33] The decision of advertising partners to divert adverts away from the site is voluntary.

2.1.4. Website-blocking injunctions - copyright, intellectual property and defamation

---

27 See *Nominet* website, *Terms and Conditions of Domain Name Registration*, available at http://www.nominet.org.uk/uk-domain-names/registering-uk-domain/legal-details/terms-and-conditions-domain-name-registration (26.03.2015).

28 See *Nominet* website, [*Draft*] *report of the Stakeholder Group "Domain names used in connection with criminal activity"* (undated), available at http://www.nominet.org.uk/sites/default/files/Report%20of%20the%20Nominet%20Stakeholder%20Group%20draft%200%202%202.pdf (26.03.2015).

29 City of London Police website, *PIPCU*, available at https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/default.aspx (21.04.2016).

30 The Intellectual Property Office is the official UK government body responsible for intellectual property rights including patents, designs, trademarks and copyright.

31 City of London Police website, *Operation Creative and IWL*, available at https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx (21.04.2016).

32 ALPHR.com, *Policing the web: anti-piracy and beyond*, interview with Detective Chief Inspector Andy Fyfe, 22nd September 2014, available at http://www.alphr.com/news/390670/policing-the-web-anti-piracy-and-beyond (21.04.2016).

33 It is reported, pursuant to a Freedom of Information Act request that, of the 75 requests sent to domain name registrars to suspend domain names at that time, only five had been granted: Torrentfreak.com website, *Domain Registrars deny police requests to suspend pirate sites*, August 8th 2014, available at https://torrentfreak.com/domain-registrars-deny-police-requests-suspend-pirate-sites-140808/ (21.04.2016). By August 2015, police had sent out suspension requests for 317 domain names: Torrentfreak.com website, *UK Piracy police asked domain registrars to shut down 317 sites*, August 21st 2015, available at https://torrentfreak.com/uk-piracy-police-asked-domain-registrars-to-shut-down-317-sites-150821/ (21.04.2016).

Court orders known as "**injunctions"** are increasingly being used to require ISPs to block material on the internet produced by third parties, particularly in the areas of copyright, defamation and privacy law.[34] Safeguards are usually contained in the wording of the orders themselves, agreed on a case-by-case basis.

In the field of **copyright law**, **section 97A of the Copyright, Designs and Patents Act 1988**[35] provides the High Court with the **power to grant an injunction** against an ISP to block access to the internet or particular sites where that ISP has actual knowledge of a person using their service to infringe copyright.[36] Over the past three years, a series of orders have been made in cases involving the major UK ISPs as defendants (who, together, have a market share of some 95% of UK broadband users), where typically now, they do not oppose the application for an order, but instead, seek to negotiate the wording of the order. Such actions, brought by the rights holders themselves, have resulted in a list of more than a hundred websites, which ISPs are required to prevent their users from accessing.[37] Section 97A was first successfully secured in a group of cases which have come to be known as the *Newzbin cases. Twentieth Century Fox Studios* relied on section 97A to obtain an injunction against ISP, British Telecom ("BT"), to block its customers' access to a version of the *Newzbin* online service used for mass copyright infringement.[38]

An ***Anti-piracy Code*** **had been previously proposed** under provisions of the Digital Economy Act 2010 with the aim of combatting online copyright infringement by internet users.[39] This would have required large ISPs ultimately to block or suspend access to the internet by subscribers whose accounts were found to have been used to breach copyright laws (such as by illegally downloading movies and music). However, secondary legislation for implementing the *Code* was subsequently withdrawn in July 2014 favour of a **voluntarily agreed framework** by the rights holders and ISPs simply designed to educate alleged infringers about the harm of piracy.[40] No details of the voluntary system, entitled "*Creative Content UK",* have yet been published, but it is not anticipated that

---

34 An injunction is an equitable remedy, being a remedy that originated in the English courts of equity. Described in the *Oxford Dictionary of Law* (ed. Jonathan Law, 7th ed., Oxford, 2009, p.204) as, "*that part of English law originally administered by the Lord Chancellor and later by the Court of Chancery, as distinct from that administered by the courts of common law. The common law did not recognise certain concepts and its remedies were limited in scope and flexibility, since it relied primarily on the remedy of damages.*"

35 Copyright, Designs and Patents Act 1988, available at http://www.legislation.gov.uk/ukpga/1988/48/contents (26.03.2015).

36 It is partly because of the availability and successful use of this remedy, that **section 17 of the Digital Economy Act 2010**, which provided for a further power for a blocking injunction, "*in respect of a location on the internet,"* was never implemented through the adoption of secondary legislation and was recently repealed by the Coalition Government.

37 See, by way of example, the orders to which ISP Sky Broadband is subjected to, available at http://help.sky.com/articles/websites-blocked-under-order-of-the-high-court (25.03.2015).

38 In the case of *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc* [2011] England and Wales High Court 1981 (Chancery Division) available at http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html (08.04.2015).

39 See Office of Communications (Ofcom), *Online infringement of copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial* obligations, 26 June 2012, available at http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf (26.03.2015).

40 See UK Government press release, *New education programme launched to combat online piracy*, available at https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy (26.03.2015).

subscribers would be exposed to the risk of having their service suspended or blocked on a permanent basis.

For the first time, in October 2014, an application for a website-blocking order was brought against UK ISPs in order to combat **trademark infringement**.[41] With no statutory counterpart in the field of trademarks to section 97A of the 1988 Act, the High Court relied on a **general legislative power to issue an injunction**, "*in all cases where it appears to be just and convenient to do so*".[42] In this case, the power was relied on to specifically order UK ISPs to block access to a range of web addresses for replica *Richemont* brands, including www.hotcartierwatch.com, www.cartierlove2u.com and www.montblancoutletonline.co.uk.

Under English law, **protection against defamation** derives from common law.[43] One of the long-established available remedies is a **permanent injunction** against a defendant to prevent further publication of the defamatory material. However, as from 1st January 2014, the Defamation Act 2013[44] removed the jurisdiction of courts in England and Wales to determine defamation actions against *secondary publishers* of defamatory material (namely, those who are not the author, editor or publisher).[45]

Most online intermediaries will now usually be classified as secondary publishers and therefore no longer exposed to the possibility of being sued for defamation. However, those which engage in conduct going beyond the processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded might be treated as "editors" or "publishers" of the statement. This is particularly the case where it is said that those statements are capable of being retrieved, copied, distributed, or made available via their equipment, systems or services.[46] **Certain intermediaries, such as ISPs, are still therefore exposed to the possibility of being ordered to block sites containing defamatory material** under the terms of a permanent injunction granted to a successful claimant in legal proceedings.

Permanent injunctions cannot be granted against those who are not a party to the defamation action. However, successful claimants who have successfully sued the author of defamatory online statements may now also apply for an Order under section 13 of the Defamation Act 2013[47] compelling *any person who was not the author, editor or publisher of the defamatory statement*, to stop distributing, selling or exhibiting material contained in the statement. This is known as an "**Order to remove or cease distribution**". This latter category of "secondary publishers" may

41 *Cartier International AG and Ors v British Sky Broadcasting & Ors* [2014] England and Wales High Court 3354 (Chancery Division), available at http://www.bailii.org/ew/cases/EWHC/Ch/2014/3765.html (25.03.2015).

42 Senior Courts Act 1981, section 37(1), available at http://www.legislation.gov.uk/ukpga/1981/54/section/37 (25.03.2015).

43 Through case law such as *Parmiter v Coupland* (1840) 6 Meeson & Welsby's Exchequer Reports 105, *Youssoupoff v MGM Studios* (1934) 50 Times Law Reports 581 and *Hebditch v McIlwaine* [1894] 2 Queen's Bench 58.

44 Defamation Act 2013, section 10.

45 A number of cases (for example, *Godfrey v Demon* [1999] Entertainment and Media Law Reports 542, *Totalise v Motley Fool* [2002] Entertainment and Media Law Reports 20) had previously confirmed the possibility of hosted material being considered as published by the host, including ISPs, after the time at which the material has been brought to its attention.

46 An ISP that, for example, had in place systems for monitoring, moderating or censoring the content of material hosted on its servers might, depending on the circumstances, have assumed editorial or equivalent responsibility for the content of particular statements or the decision to publish them (see M. Collins, *Collins on Defamation*, Oxford University Press 2014, p. 37).

47 See section 2.2. below of this report.

potentially include a broader range of online intermediaries beyond website operators, such as ISPs. No known specific case law is yet available on this point.

Although there are no specific safeguard requirements contained in the legislation providing for the above injunctions, the text of the orders approved by the High Court in recent copyright and trademark cases typically contains **safeguards against abuse**. 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.[48]

The case of ***Cartier International AG and Ors v British Sky Broadcasting & Ors***[49] in October 2014 introduced further **safeguards.** First, it was held that future orders should also expressly permit affected subscribers of the ISP to apply to the Court to discharge or vary the orders.[50] Secondly, it is advised that the page displayed to users who attempt to access blocked websites should state not merely that access to the website has been blocked by court order, but should also 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.[51] In certain cases, it may also be appropriate to incorporate a "sunset clause", 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.

2.1.5. Website-blocking injunctions – privacy law

There are **no known legal rules** in the UK which specifically require the blocking or filtering of internet content by internet access providers **in the fields of privacy law**. There is nevertheless the potential for an internet access provider, in the right circumstances, to be subjected to a High Court injunction, requiring them to block or filter access to web pages, which, for example, misuse private information.[52] Certain **injunctions** may nevertheless place an **indirect requirement on such ISPs, as third parties, to block access to the internet** where websites to which they provide access contain the offending material. Two kinds of injunction in the field of privacy law are worth mentioning.

The first, granted only on very rare occasions, is known as a "***contra mundum* injunction"**, being a court-ordered injunction against the world at large, and not merely against the defendants to the proceedings. Depending on the wording of the injunction itself, this can provide a strong incentive in certain cases for an ISP to block websites containing the material which forms the subject of the injunction, where the ISP wishes to avoid liability for breach of the injunction.

---

48 *Cartier International AG and Ors v British Sky Broadcasting & Ors, op. cit.,* at para. 262.

49 *Ibid.*

50 *Ibid,* at para. 263. Indeed, by way of example, Sky Broadband now acknowledges this right on its webpages. See http://help.sky.com/articles/websites-blocked-under-order-of-the-high-court (25.03.2015).

51 *Ibid*, at para. 264. These safeguards were repeated in the most recent example of a s.97A order, in *1967 Limited and Ors v British Sky Broadcasting Limited and Ors* [2014] England and Wales High Court 3444 (Chancery Division), available at http://www.bailii.org/ew/cases/EWHC/Ch/2014/3444.html (25.03.2015), at para. 29.

52 However, this will more commonly be an injunction against the perpetrator themselves, where UK-based, to remove the offending material. For more detail on injunctions in the field of information and privacy rights, see section 2.2. of this report below regarding the exposure of internet host providers.

A famous example is the 2001 case[53] of claimants, Robert Thompson and Jon Venables, convicted, at the age of 11 years old, of killing the toddler, James Bulger. They were granted an injunction restraining the publication of information that would reveal their new identity or whereabouts on their release from prison at the age of 18. The injunction, deemed necessary to protect the claimants' right to life and freedom from persecution was issued not just against the newspaper defendants, but against the world at large. There was a clear possibility that an ISP could be in breach of this order if a third party posted material to its servers, even though the ISP did not know it was there. As a result, the order issued was varied by the insertion of a proviso, clarifying that an ISP (and its employees) would not be in breach of the injunction unless it had actual or constructive knowledge of the material on its servers and had failed to take reasonable steps to prevent the publication.

The second kind of injunction which can result in an obligation on an ISP to remove material is a temporary remedy, known as an "***interim injunction***". Although addressed to particular defendants, rather than being an injunction *contra mundo*, third parties, such as ISPs, can be in contempt of court[54] if they aid and abet a defendant to breach that order. Under what is known as the *Spycatcher* principle, an interim injunction prevents a person from disclosing private and/or confidential information, but also prevents third parties from disclosing the information, provided they have been given notice of the injunction. The principle is based on the notion of maintaining privacy and preserving the status quo until the conclusion of full court proceedings (in the context of ISPs, most likely to be in cases of defamation and privacy) – often concerning the material in question. Although the *Spycatcher* principle arose in the context of newspapers who had full editorial control over the contents of their publications, claimants may seek to serve such an injunction not just on traditional ISP hosts and access providers, but also on a wide variety of online intermediaries, including search engines.[55]

2.1.6. Voluntary adult content filtering

Apart from the filtering of illegal content and court-ordered website blocking, **UK ISPs make parental control services available to their subscribers** for the purpose of blocking adult and age-restricted material from the internet. The four main ISPs, Sky, BT, TalkTalk and Virgin committed to offering new customers by the end of 2013 an enforced choice at the point of purchase, installation or activation of their service as to whether or not to use the controls provided by the ISP to filter access to the internet.

By February 2014, all main ISPs had implemented this network level filtering of content, making it an **"unavoidable choice" for parents to set up internet controls**. It is however, reported that the take up rate for these parental control services amongst new customers is very low.[56]

2.2. Take-down/removal of illegal Internet content

Many of the mechanisms relied on for blocking internet content are also used to take-down or otherwise remove illegal internet content. To our knowledge, there are only **two areas in which there are statutory "notice and take-down" procedures** for the removal of illegal internet content: first, in relation to material which constitutes offences under the **Terrorism Act 2006**, and secondly,

---

53 *Venables v News Group Newspapers Ltd* [2001] 1 All England Law Reports 908.

54 'Contempt of court' in this context refers to disobedience of a court order or process.

55 See Graham J H Smith, *Internet Law and Regulation,* 4th ed., Thomson Sweet & Maxwell, 2007, p. 392.

56 See Office of Communications, *Ofcom Report on Internet safety measures*, 22 July 2014, available at http://stakeholders.ofcom.org.uk/binaries/internet/internet_safety_measures_2.pdf (26.03.2015), p.17.

under the **Defamation Act 2013**, in connection with a relatively new defence available to website operators who host potentially defamatory material.
Although there are **no other statutory provisions in either criminal law or civil law** which provide for the removal of illegal internet content, it is reported that **many hosts remove such material regardless of the legitimacy of the complaint**, in order to better avoid being held liable.[57] In practice, many ISPs, including website hosts and social networks, have **"acceptable terms of use" policies** or "Community Guidelines", under which they do not tolerate any material which may offend or hurt people. Such material is usually quickly taken down following the receipt of a complaint.

The **Electronic Commerce (EC Directive) Regulations 2002**[58] (the "E-Commerce Regulations") incorporate into UK law the European Union's E-Commerce Directive,[59] and provide defences for ISPs, including hosts, against liability for potentially illegal internet content, where they have actual or constructive knowledge of it and remove or disable access to the material.[60] According to a number of commentators, these rules, in the absence of specific notice and takedown provisions, **act as strong additional incentive to ISP hosts** to remove, rather than to leave up, potentially illegal material.[61]

2.2.1. Takedown/removal of child abuse and obscene adult content

For UK-hosted content within the IWF's remit,[62] such as child abuse images, the IWF operates a **Code of Practice for Notice and Takedown**.[63] Notices are only issued where the IWF believes that material would be capable of sustaining a criminal prosecution if it were to be put before a jury. Upon receipt of a Notice from the IWF, a member ISP host must either act expeditiously to remove the notified content or notify the IWF if the Notice appears to have been improperly issued.[64] This requirement is supported by the ISPA, whose Code of Practice requires its members to act in accordance with IWF Notices to remove illegal child abuse images, even if they are not members of the IWF.[65]

---

57 See, for example, E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation, op. cit.*, p. 320.

58 Electronic Commerce (EC Directive) Regulations 2002 (Statutory Instrument 2013/2002), available at http://www.legislation.gov.uk/uksi/2002/2013/contents/made (31.03.2015).

59 Electronic Commerce Directive 2000/31/EC.

60 Electronic Commerce (EC Directive) Regulations 2002, *op. cit.*, regulation 19.

61 See, for example: Daithi Mac Sitigh, *The fragmentation of intermediary liability in the UK,* Journal of Intellectual Property Law & Practice 2013, Vol. 8, No. 7, 521-531 at 525; E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation, op. cit.*, p. 320; C. Ahlert, C. Marsden, C. Yung, *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, (undated) p. 27, available at http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf (31.03.2015).

62 See section 2.1.1. of this country report, above. It is reported that the UK continues to host just a small volume of online child sexual abuse content (0.3% in 2014). Nevertheless, this translated into the issuing of 51 takedown notices to remove images hosted in the UK on 95 URLs. 43% of webpages are removed in 60 minutes or less and 100% are removed within 4 days (see IWF, *Annual Report 2014*, *op. cit.*, pp.11-12).

63 IWF, *Code of Practice*, available at https://www.iwf.org.uk/members/member-policies/funding-council/code-of-practice#F1 (31.03.2015).

64 *Ibid,* section 5.

65 ISPA *Code of Practice, op. cit.,* section 5.4.

By way of a safeguard, the **IWF's Code of Practice contains an Adjudication Process** relating to breaches of the Code, under which the Chief Executive of the IWF will investigate suspected breaches and examine whether any such Notice has been issued incorrectly.[66]

Where content has been traced to a location outside of the UK,[67] data is uploaded to the INHOPE[68] database (where there is an INHOPE hotline in the host country) or the relevant country's police are notified. It is reported that in 2014, 84% of URLs hosted outside the UK were removed within 10 days.

2.2.2. Takedown/removal of material encouraging terrorism

The **Terrorism Act 2006 provides a "notice and takedown" procedure**,[69] under which ISP hosts can be required, on notice from the police, to take down material supportive of terrorism. Where they fail to do so, they risk being regarded as having endorsed such material and can be held criminally liable for it.[70] It is reported that the removal of unlawful terrorist content, **in practice, takes place through informal contact** between the police and ISPs and that it has never been necessary to rely on these formal requirements.[71]

2.2.3. Public order and targeted communications offences

Insofar as the prevention of disorder or other crime is concerned, there are **no legal rules requiring ISPs to remove potentially illegal content**. However, in relation to certain public order offences of stirring up hatred on the grounds of religion or sexual orientation,[72] Statutory Regulations[73] have been implemented, consistent with the wording of the E-Commerce Regulations, which create specific **exemptions from criminal liability for ISP hosts** (as well as for "mere conduits" and "caches") where they, "*expeditiously remove the information or disable access to it,*" in circumstances where they have actual knowledge of the relevant material, that it was threatening and was intended to stir up religious hatred or hatred on the grounds of sexual orientation.

Generally speaking, existing public order laws and laws designed to regulate harmful messages have been used to prosecute only those directly responsible for the criminal acts themselves. Section 4A of the **Public Order** Act 1986,[74] for example, provides that it is an offence for a person to use,

---

66 IWF, *Code of Practice, op. cit.,* section 8.

67 As was the situation in 99.7% of cases in 2014 – see IWF *Annual Report 2014*, *op. cit.*, p. 11.

68 INHOPE describes itself as, "*an active and collaborative network of 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the internet*". See INHOPE website, *Who We Are*, available at http://www.inhope.org/gns/who-we-are/at-a-glance.aspx (10.11.2015).

69 See section 2.1.2. above of this country report.

70 The Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 (available at http://www.legislation.gov.uk/uksi/2007/1550/contents/made (31.03.2015)) were also implemented to clarify that ISPs will be exempt from criminal liability where they respect provisions of the E-Commerce Regulations in relation to offences under the Terrorism Act 2006 (including, for hosts, expeditiously removing the information or disabling access to it).

71 House of Lords question to Government, Hansard citation: House of Lords Debate, 23 September 2013, c421, available at They Work For You website, *op. cit.*

72 See information on the Public Order Act 1986, below.

73 The Electronic Commerce Directive (Hatred against Persons on Religious Grounds or Grounds of Sexual Orientation) Regulations 2010, Regulation 7, available at http://www.legislation.gov.uk/uksi/2010/894/regulation/7/made (31.03.2015).

74 Public Order Act 1986, available at http://www.legislation.gov.uk/ukpga/1986/64 (31.03.2015).

"*threatening, abusive or insulting words or behaviour,"* or to display, *"any writing, sign or other visible representation which is threatening, abusive or insulting,"* which causes, *"that or another person harassment, alarm or distress,*" and which the speaker intends to have that effect. As mentioned above, further offences are provided for where expression is likely to incite hatred on the grounds of race, religion and sexual orientation.[75] **Various individuals have been successfully prosecuted i**n recent years under this provision in relation to material posted on the internet.

Similarly, laws on **targeted communications**, such as the Malicious Communications Act 1988[76] and the Protection of Harassment Act 1997,[77] initially designed to tackle poison pen letters, offensive phone calls and stalking, have since been applied to digital communications. More recently, section 127 of the Communications Act 2003[78] was introduced to make it a specific offence to send or cause to be sent through a *public electronic communications network*, "*a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.*"

In the absence of the necessary intent to cause a criminal offence however, it is generally considered **unlikely that an ISP host will be held criminally liable for unlawful content** communicated by a third party. Prosecuting Guidelines[79] issued by the Crown Prosecution Service on cases involving communications sent via social media do not appear to envisage the prosecution of anyone other than those directly responsible for the offending material. In practice, it would appear that potentially criminal material is not removed by ISP hosts pursuant to criminal court proceedings, but rather, at an early stage, in accordance with Acceptable Terms of Use policies and/or to avail themselves of the exemptions from criminal liability deriving from the E-Commerce Regulations.[80]

2.2.4. Takedown/removal of defamatory statements

In the area of **defamation law**,[81] a new piece of primary legislation, the **Defamation Act 2013**, includes a provision, section 13(1), aimed at "the **operator of a website**". This permits successful claimants in defamation cases to apply for **an order compelling the operator of a website to remove a statement posted on the website** (an "Order to remove or cease distribution"). This applies where the court has found such statement by the author to be defamatory and therefore unlawful. Such an order may be made even in cases where the statement was not posted by the operator, and the operator was not a defendant in the action.[82]

---

75 Public Order Act 1986, sections 29B-G.

76 Malicious Communications Act 1988, available at http://www.legislation.gov.uk/ukpga/1988/27/contents (31.03.2015).

77 Protection from Harassment Act 1997, available at http://www.legislation.gov.uk/ukpga/1997/40/contents (31.03.2015).

78 Communications Act 2003, section 127, available at http://www.legislation.gov.uk/ukpga/2003/21/section/127 (31.03.2015).

79 Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media*, available at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html (31.03.2015).

80 Even *True Vision,* the website set up by the Association of Chief Police Officers to allow people to report hate crime, including that found online, encourages victims in the first instance, to report offending material to the website administrator or the hosting company. See Report-it.org, *Internet Hate Crime*, available at http://report-it.org.uk/reporting_internet_hate_crime and section 4 of this country report below. See also See, HM Government, *Challenge it, Report it, Stop it – Delivering the Government's hate crime action plan*, *op. cit.* p. 7.

81 For more information on 'defamation' under the English common law, see section 2.3. below.

82 Defamation Act 2013, section 13, available at http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted (31.03.2015).

As to legal actions for defamation brought against the operator of a website, section 5(1) of the Defamation Act 2013 allows such an operator **a defence where it simply shows that it was not responsible for posting the statement on the website**. Section 5(3), however, enables the defence to be defeated if the claimant has not been able to identify the person who posted the statement, and where "*the claimant gave the operator a notice of complaint in relation to the statement, and the operator failed to respond to the notice of complaint in accordance with any provision contained in the [Defamation (Operators of Websites) Regulations 2013].*"

The **Defamation (Operators of Websites) Regulations 2013**[83] is a piece of accompanying secondary legislation which sets out a 48-hour window during which the website operator must act in order to continue to be afforded the **protection of the statutory provision against any future court action for defamation**. Generally speaking however, where the operator passes on a notice of complaint to the poster, and complies with certain requirements, it is not then required to take material down in order to benefit from the defence. On the other hand, where it has no means of contacting the poster, where the poster fails to respond, or where the poster's response does not meet requirements, **the operator must remove the statement** in order to maintain protection from liability.[84]

A number of **important cases** have focused on the liability of ISP hosts for defamatory third-party content, rather than any obligations to remove the material. In 2001, in the case of *Godfrey v Demon Internet Service*,[85] it was found that it was possible for an ISP to be liable for the content of sites which it hosts; in 2006, in *Bunt v Tilley*,[86] the High Court rules that ISPs have a qualified immunity for defamatory material so long as they do not provide an editorial function; and in 2011, in ***Tamiz v Google Inc***,[87] the Court of Appeal found that Google, as the provider of an internet platform for blogging could not be regarded as a publisher, but could be held responsible once it had been put on notice of the defamatory postings and had had a reasonable time to remove it.

With the introduction of the Defamation Act 2013 on 1st January 2014 however, section 10 now specifically provides that **courts no longer have jurisdiction to hear and determine defamation actions** brought against anyone, "*who was not the author, editor or publisher of the statement complained of, unless the court is satisfied that it was not reasonably practicable for an action to be brought against the author, editor or publisher.*" In other words, it is likely that courts may only entertain defamation actions against an ISP where it was the direct author, editor or publisher of the allegedly defamatory statement or where it was not possible to sue the actual author, editor or publisher. The **earlier case law on liability is therefore of limited value**. This does not detract in any way from the rules on orders against website operators to remove defamatory statements, and, where ISPs may be sued for defamation (usually where it is not reasonably practicable for an action to be brought against the actual author of the statement), they may still be able to avail themselves of the defence under section 5 of the Defamation Act 2013.

2.2.5. Takedown/removal of private or confidential information

---

83 The Defamation (Operators of Websites) Regulations 2013, available at http://www.legislation.gov.uk/uksi/2013/3028/contents/made (22.01.2015). See also Ministry of Justice issued guidance "*Complaints about defamatory material posted on websites: Guidance on Section 5 of the Defamation Act 2013 and Regulations*", January 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/269138/defamation-guidance.pdf (22.01.2014).

84 The Defamation (Operators of Websites) Regulations 2013, *ibid*, Schedule, sections 2-6.

85 *Godfrey v Demon* [1999] Entertainment and Media Law Reports 542.

86 *Bunt v Tilley* [2006] England and Wales High Court 407 (Queen's Bench Division).

87 *Tamiz v Google Inc* [2013] England and Wales Court of Appeal Civil Division 68.

There is **no UK legislation directed at ISP hosts** which requires them to remove or take down third party material which breaches the privacy rights of individuals or businesses. Until recently, there was not even a right (common law or statutory) to privacy under English law. However, the implementation of the Human Rights Act 1998 ("HRA") in 2000 resulted in rights of the European Convention on Human Rights ("ECHR") being given direct effect under UK law. This allows individuals and businesses to apply to the High Court for a **"privacy injunction" under Article 8 of the ECHR** to prevent the publication of private or confidential information. Between 2009 and 2011, a number of privacy injunctions had successfully been obtained by high profile individuals, including what became known as "super injunctions" preventing publication of details of the identity or existence of the injunction. These were largely undermined by social network users, such as those on *Twitter*, who effectively acted in contempt of court by sharing details of the material in question.[88] A **Parliamentary inquiry** was therefore set up in 2011 to determine whether legislation was needed to address the issue.[89] This concluded that the current approach, where judges balance the evidence and make a judgment on a case-by-case basis, provides the best mechanism for balancing Article 8 and Article 10 ECHR rights.

Having taken evidence from expert witnesses, it was reported by the Parliamentary Committee that UK-based **ISP hosts normally await notice from a court or other official entity** before reactively **taking down material** which infringes privacy.[90] Often however, the ISP host will be based in a foreign jurisdiction, which is not subject to UK law. Nevertheless, the Committee encouraged social media providers to disseminate best practice and discourage illegality amongst users, whilst also recommending that courts be proactive in directing claimants to serve notice of injunctions on internet content platforms. It noted that in the meantime, *Twitter* had introduced a policy allowing it to filter content on an "in-country" basis, allowing it to take down content in one country, whilst leaving it available to users in other parts of the world.[91] Although it is therefore not possible to enforce the terms of a privacy injunction against a non-UK based ISP host, it appears that in practice, certainly the larger social network platforms are making increasing efforts to assist in the implementation of such injunctions with regard to content posted by their users.

Finally, in the field of **data protection law**, it should also be noted that under section 14 of the Data Protection Act 1998,[92] if a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the **court may order the data controller** (such as the website operator of the website on which the data appears) t**o rectify, block, erase or destroy those data** and any other personal data in respect of which he is the data controller, and which contain an expression of opinion which appears to the court to be based on inaccurate data.

---

88 "Contempt of court" in this context refers to disobedience of a court order or process.

89 Joint Committee on Privacy and Injunctions, *Privacy and Injunctions, Session 2010-2012*, HL Paper 273, HC 1443, 27 March 2012, available at http://www.publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/273.pdf (01.04.2015).

90 *Ibid,* para. 105. As to search engines such as *Google*, however, the Committee acknowledged that there could be countless offending items which would each require a separate notice for removal to take place. Controversially, it recommended that Google and other search engines should take steps to actively develop technology to automatically remove offending material in order to ensure that their websites are not used as vehicles to breach the law.

91 *Ibid,* para. 108.

92 Data Protection Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/29/contents (02.04.2015).

3. Procedural Aspects

3.1 Child abuse and obscene adult content

The **Internet Watch Foundation ("IWF")[93] is recognised as the regulatory authority** for blocking, filtering and removal from the internet of child abuse material. Set up in 1996 pursuant to an agreement between the Government, police forces and the Internet Service Provider ("ISP") industry, it operates a "hotline" to allow members of the public to report potentially illegal images. Since April 2014, the IWF also began **proactively searching for child sexual abuse images and videos**. This is said to have resulted in the processing of 45% more reports than in 2013.[94]

Determining whether imagery is to be included on the IWF's blacklist initially involves an **assessment by IWF experts** of the content, in line with the UK Sentencing Council Guidelines for the Sexual Offences Act 2003.[95] These broadly divide child sexual abuse imagery into three categories, with categories A and B being images involving sexual activity and Category C being other indecent images not falling within categories A or B. Every analyst is required to obtain a mandatory second opinion from the hotline manager before concluding that he or she is dealing with a category C image.[96] In assessing content, the IWF also considers the potential problems ("identified risks") caused by addition of the *URL* to the blacklist to Internet users, licensees and the impact on the website owner's reputation.

Action is initially taken to **seek removal at the source of the content**. If the content is hosted in the UK, the IWF will contact relevant law enforcement agencies and subsequently notify the hosting provider with a request to remove the content. In 2014, it was reported that 43% of such content was removed within 60 minutes or less, and all content was removed within 4 days. Where, as is more likely, content is hosted abroad, the IWF passes on the intelligence to the relevant hotline or police body in the hosting country.[97] As it can often take several days or weeks before content is removed at source in the hosting country, the IWF will add the relevant *URL* depicting child sexual abuse material to their blacklist until the content is removed The IWF blacklist is updated twice daily at 12 noon and 5pm.[98]

On release of the updated blacklist to its members, many ISPs will block access to the content by way of the ***Cleanfeed* system**, a technical system developed by British Telecom ("BT") and implemented by a number of ISPs.[99] It is reported that the design of the *Cleanfeed* system has not been disclosed by BT,[100] and that each of the ISPs regards the technical and commercial details of these systems as

---

93 See section 2.1. of this country report above for more information.

94 IWF, *Annual Report 2014*, *op. cit.*, p. 5.

95 IWF, *URL List Policies, Procedures and Processes*, available at https://www.iwf.org.uk/assets/media/members/URL%20List%20policies%20procedures%20and%20processes%20FINAL%202.pdf (01.04.2015).

96 See IWF, *Independent Inspection Report 2015*, available at https://www.iwf.org.uk/assets/media/accountability/IWF%20Independent%20Hotline%20Audit%202015.pdf (11.11.2015), para. 12.

97 See section 2.2.1. above of this country report on the role of IHOPE.

98 IWF, *Independent Inspection Report 2015*, *op. cit.*, para. 14.

99 The technological systems used by the different ISPs were discussed by Justice Arnold in the October 2014 case, *Cartier International AG and Ors v British Sky Broadcasting & Ors* [2014] England and Wales High Court 3354 (Chancery Division), *op. cit.,* at paras .38-51. *Sky*, for example, uses a system known as *Mohawk*; *TalkTalk* uses Detica and *Virgin* uses *Web Blocker*.

100 See Open Rights Group, *Cleanfeed*, available at https://wiki.openrightsgroup.org/wiki/Cleanfeed (01.04.2015).

sensitive confidential information. This is however described as a two-stage IP address re-routing and Deep Packet Inspection ("*DPI*") based *URL* blocking system capable of blocking websites that hosted on shared IP addresses without blocking other websites hosted at the same address.[101]

If any party with a legitimate association with the content or a potential victim, hosting company, publisher or internet consumer is unhappy about the IWF's assessment of content regarding a notice to remove that content, or about the inclusion of a *URL* on the IWF's blacklist, they may make a complaint. Such **appeal will be re-assessed by an IWF Manager**, and if the original decision is upheld, the complaint may then be **referred to the relevant police agency** for assessment should the appellant wish to continue their appeal.[102] There is no information available on the nature of the review by the relevant police agency. Following assessment by the police agency, the appellant is informed and, since 2014, now has a further right of appeal to an "appeal tribunal" of the IWF, chaired by a retired judge.[103]

3.2 Material encouraging terrorist activity

The **Counter Terrorism Internet Referral Unit ("CTIRU")** is a dedicated police unit which assesses and investigates internet-based content which may breach the Terrorism Act 2006. Members of the public who are concerned about such material can make referrals to the CTIRU through the gov.uk website, https://www.gov.uk/report-terrorism.

Section 3 of the Terrorism Act 2006[104] sets out a **notice and take-down procedure**. This requires a police constable to give notice to the "relevant person", usually the operator of the site on which the material has appeared. This declares that in the opinion of the constable giving it, the statement or the article or record is unlawfully terrorism-related. The notice broadly requires the relevant material to be removed from public access or is appropriately modified, and that a failure to comply within two working days will result in the material being regarded as having that person's endorsement.

It is reported by the UK Government that **in practice** however, the CTIRU has never had to rely on the notice and take-down procedure, and that **ISPs cooperate willingly**.[105] Blocking of web pages by internet access providers is understood to take place using the same technology operated for implementing the IWF blocking regime (see 3.1.above). There is **no known formal appeals process**.

3.3 Other criminal material

There are no legal rules regulating the blocking, filtering or taking down of material which potentially amounts to a criminal offence, such as public order, hate crime or targeted communications.[106] In practice, it is the **internet access providers and ISP hosts** themselves which police such material. Content is removed on a case-by-case basis, either upon request from the police or simply in

---

101 See *Cartier International AG and Ors v British Sky Broadcasting & Ors, op. cit.,* at paras 42-43.

102 See IWF, *Content Assessment Appeal Process,* available at https://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process (01.04.2015).

103 See section 5 of this country report, below.

104 Terrorism Act 2006, section 3, available at http://www.legislation.gov.uk/ukpga/2006/11/section/3 (02.04.2015).

105 See earlier response of Lord Taylor of Holbeach to Parliamentary questions, Hansard citation: House of Lords Debate, 23 September 2013, c421, *op. cit.*

106 See section 2 above of this country report.

accordance with their own "Acceptable Terms of Use" policies; these often contain lower thresholds as to what constitutes unacceptable material than that tolerated by criminal laws.[107]

3.4 Domain name abuse

Nominet is acknowledged by the UK Government as the **UK's internet registry** for "*uk*" domain names.[108] Describing itself as a not-for-profit private, public-purpose, company, it enters into a **contract of registration** with anyone who registers a domain name ending in "*uk*". *Nominet* reserves the right, in its contract of registration, to cancel the domain name if any condition is broken by the domain name user, including that such user is entitled to register the domain name and that the domain name is not used for any unlawful purpose.[109]

Nominet operates a "***Dispute Resolution Service Policy***"[110] and accompanying "*DRS Procedure*"[111] under which the person in whose name a domain name is registered must submit to proceedings where someone complains that the domain name amounts to an abusive registration.[112] The person in whose name the domain name is registered must be sent the complaint by *Nominet* in accordance with the *DRS Procedure*.[113]

An appointed **independent expert will be appointed to adjudicate the dispute** if the parties are unable to resolve matters through informal mediation, and he or she can ultimately decide to cancel or suspend the domain name registration.[114] Such decision is implemented by *Nominet* making any necessary changes to its domain name register database after 10 days of the date that the parties to the dispute were notified. The decision must be communicated to both parties within 3 days of receipt by *Nominet* of the decision of the expert.[115] Both parties have a **right of appeal**, which is considered by a panel of an independent "*Expert Review Group*"[116]

As to the process followed by the Police Intellectual Property Crime Unit ("PIPCU") in disrupting the running of sites determined as breaching copyright under the Operation Creative program, there is no such formal process. It is pointed out by the PIPCU that the placing of a website on the Infringing Website List ("IWL") does not, in any event, mean that such website is automatically blocked, but

---

107 See, for example, the *Sky* Broadband *Acceptable Use Policy ("AUP")*, which refers to the ability of *Sky* to block any electronic communication that they consider to have breached the AUP. A breach includes material which not only violates any law, but which, "*promotes or encourages illegal or socially unacceptable or irresponsible behaviour*." Available at http://www.sky.com/shop/terms-conditions/broadband/usage-policies/ (02.04.2015).

108 See section 2.1.3. above of this country report for further information.

109 See Nominet, *Terms and Conditions of Domain Name Registration*, *op. cit.,* conditions 7 and 16.

110 Nominet, *DRS Policy*, available at http://www.nominet.org.uk/disputes/when-use-drs/policy-and-procedure/drs-policy (02.04.2015).

111 Nominet, *DRS Procedure*, available at http://www.nominet.org.uk/disputes/when-use-drs/policy-and-procedure/drs-procedure (02.04.2015).

112 "Abusive registration" is broadly defined as meaning that the name has been registered primarily for the purposes of transferring the domain name to the complainant, as a blocking registration against a name or mark in which the complainant has rights or for the purpose of disrupting the business of the complainant. (clause 3, *ibid*).

113 Nominet, *DRS Procedure, op. cit.*, section 2.

114 Nominet, *DRS Procedure*, *op. cit.*, section 17(c).

115 *Ibid*, section 17(a).

116 Nominet, *Expert Review Group*, available at http://www.nominet.org.uk/disputes/resolving-domain-disputes/how-it-works/expert-review-group (02.04.2015).

rather that the advertising industry which subscribe to the list may voluntarily choose to divert adverts away from that site.

The first step is for a copyright holder to complete an online referral form to enable PIPCU to carry out a full assessment of the circumstances of their case.[117] In the absence of any formal publicised procedure, it is understood from the PIPCU web pages and other anecdotal information,[118] that PIPCU will then make contact with those responsible for the website to cooperate with officers' enquiries and, if necessary, to cease their behaviour. In the absence of a positive response, PIPCU then approach the domain name registrar and host and ask for them to consider taking down the website. Only if there is again no positive response, does PIPCU take the decision to place the website on the IWL. There is no further right of appeal against this decision.

3.5 Website blocking and take-down injunctions

The legal mechanism for blocking, filtering and take-down of internet content which is defamatory, breaches copyright, trademarks or privacy laws will usually be by way of an **injunction issued (in England and Wales) by the High Court**.[119]

Implementation of the decision **will depend on the wording of the injunction** itself, and this will vary according to the nature of the infringement and the facts of each case in which an injunction is sought. However, in the October 2014 trademark infringement case of *Cartier International AG and Ors v British Sky Broadcasting & Ors*,[120] the Judge provided an example of the wording used in section 97A copyright blocking injunctions ("section 97A orders"), setting out how ISPs are to implement the blocking of access. The precise wording, he noted, would vary from ISP to ISP to take account of the different technologies they employ, but the general form of the orders is substantially the same.[121] Referring to the section 97A orders obtained to date in England and Wales, the standard text of the handful of provisions usually adopted in such cases is set out. The principal provision is as follows:

> "1. In respect of its residential fixed line broadband customers to whose service the system known as …. Is applied, the … Defendant [ISP] 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 or 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….."[122]

---

117 City of London Police website, *PIPCU Referral Guide,* Intellectual Property Office, available at https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Documents/pipcu-referral-guide.pdf (25.04.2016).

118 ALPHR.com, *Policing the web: anti-piracy and beyond*, interview with Detective Chief Inspector Andy Fyfe, *op. cit.* See also City of London Police, *Operation Creative and IWL*, available at https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx (25.04.2016).

119 In England and Wales, it is, broadly speaking, in the High Court of Justice rather than the country court (the lower civil law court) that legal claims in these fields will be launched. Insofar as injunctions in copyright cases are concerned, section 97A of the Copyright Designs and Patents Act 1988 states that "*The High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider….*" As for defamation, under section 18 of the County Courts Act 1984, unless the warring parties agree to give the county court jurisdiction in their dispute, section 15 of the same Act provides that the county court does not have jurisdiction to determine any defamation action.

120 *Op. cit.* Judgment by Mr Justice Arnold.

121 *Op. cit.,* at para. 72.

122 *Ibid.*

The subsequent provisions of the injunction specify the technical system of the ISP relied on to implement the blocking of the websites identified by the claimants, and furthermore permits the operators of the "*Target Websites*" to apply on notice to vary or discharge the injunction.

Implementation of the blocking by ISPs themselves takes place using **technology operated by each ISP**. The technical and commercial details of these systems are said to be regarded as sensitive confidential information. By way of example, *Sky Broadband* uses a system known as *Hawkeye* to implement section 97A orders, while *British Telecom* uses a mixture of *Cleanfeed*[123] and *Nominum*, a Domain Name System ("*DNS*") blocking system.

In addition to permitting the ISPs to apply to the court to discharge or vary the orders in the event of any material change of circumstances and the **possibility for the operators of Target Websites to apply to the court to discharge or vary the orders**, it has recently been ruled that such orders should also permit affected subscribers of the ISPs themselves, to apply to the court to discharge or vary the orders. Furthermore, the page displayed to users who attempt to access blocked websites should no longer merely state that access to the website has been blocked by court order, but should also identify the party which obtained the order and state that affected **users have the right to apply to the court to discharge or vary the order**.[124]

Finally, where permission is given in the court proceedings to **appeal** against a decision of the High Court (otherwise known as "leave to appeal"), either party may appeal to the Court of Appeal. Such appeal will generally however only be allowed where the lower court's decision was "*wrong*" or "*unjust because of a serious procedural or other irregularity in the proceedings in the lower court*."[125] In practice however, it is reported that for section 97A orders at least, neither the ISPs nor the rights holders have appealed against any aspect of the orders made in any of the cases made requiring ISPs to block access to websites.[126]

4. General Monitoring of Internet

There is **no particular UK entity** tasked with the specific function of actively monitoring internet content for the purpose of assessing compliance with legal requirements.

Insofar as **Internet Service Providers** ("ISPs") are concerned, although Article 15 of the EU's Electronic Commerce Directive[127] (prohibiting Member States from imposing a general obligation on intermediaries to monitor the information which they transmit or store) was not transposed into the UK's Electronic Commerce (EC Directive) Regulations 2002,[128] a court would have to have regard to Article 15 when considering the grant of an injunction against an intermediary. Indeed, in the 2011 case of *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc*,[129] BT argued that the injunction against it would contravene the Directive. This required BT to prevent its subscribers from accessing "Newzbin2", which provided links to pirated films of Twentieth Century Fox. The

123 See section 3.1. of this country report above for more details.

124 *Cartier International AG and Ors v British Sky Broadcasting & Ors* [2014], *op. cit.,* at paras 262-264, also applied in *1967 Limited and Ors v British Sky Broadcasting Limited and Ors* [2014], *op. cit*.

125 Civil Procedure Rules, Part 52, rule 52.11(3), available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part52 (08.04.2015).

126 See comments of Mr Justice Arnold in *Cartier International AG and Ors v British Sky Broadcasting & Ors* [2014], *op. cit.* at para. 4.

127 2000/31/EC, *op. cit.*

128 Statutory Instrument 2013/2002, *op. cit.*

129 *Op. cit.*

injunction awarded did not require BT to actively monitor content but to block access to Newzbin2 via automated methods, which BT was already using to prevent access to child pornography. The Court said: "*To the extent that this amounts to monitoring, it is specific rather than general.*"[130]

Broadly speaking, the **review of internet content** for its compliance with legal requirements takes place, in practice, under largely **voluntary and informal notice and takedown procedures**.

In fields of private law, such as copyright, defamation and privacy law, **potentially unlawful material is usually brought to the attention** of the internet access provider or website operator by the rights holder themselves rather than through active monitoring by the intermediary.

Even where statutory notice and takedown procedures operate, such as under the Terrorism Act 2006 or the more recent Defamation (Operators of Websites) Regulations 2013, there is **no obligation on the relevant intermediary to assess whether the content is in compliance** with legal requirements. In the case of material encouraging terrorism, it has been reported[131] in any event, that the removal of online content operates in practice on an informal basis at the request of the Counter Terrorism Internet Referral Unit ("CTIRU"). **CTIRU, itself, does not actively monitor the internet** for terrorist material, but invites the public to report such content via a Government website.[132] A similar reporting system operates in relation to hate crimes, via the **Association of Chief Police Officers' *True Vision* website**.[133] There is however, no known publicly available information on the criteria relied on by the relevant law enforcement authorities for determining whether to request an ISP to remove potentially criminal online material.

The **Internet Watch Foundation's** (IWF) voluntary notice and take-down procedure regarding child pornography content also **relies on notification by internet users**, via an online "hotline". Since April 2014, the IWF says that it has also been **proactively searching for child sexual abuse images and videos**. This, it says, has led to the processing of 45% more reports of offending material than in 2013.[134] The IWF emphasises that it does not investigate material found in peer-to-peer file sharing networks. A recent Human Rights Audit commissioned by the IWF found that such a development in the IWF's work would not be appropriate, and would be better reserved for a properly trained and supervised law enforcement agency.[135]

Its competence as a relevant authority for the reporting, handling and combating of child sexual abuse images on the internet is set out in the Memorandum of Understanding[136] between the Crown Prosecution Service and the Association of Chief Police Officers. Images are **assessed by IWF staff in line with the UK Sentencing Guidelines Council's Definitive Guideline of the Sexual Offences Act**

---

130 *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc, op. cit.,* at para. 162.

131 See section 2.1.2. above of this country report.

132 Gov.uk, *Report online terrorist material*, available at https://www.gov.uk/report-terrorism (08.04.2015).

133 For further detail, see Report-it.org, *Internet Hate Crime*, available at http://report-it.org.uk/reporting_internet_hate_crime (08.04.2015).

134 IWF, *Annual Report 2014*, *op. cit.,* p.5. See also Department for Culture Media & Sport, *Press Release - Tackling illegal images – new proactive approach to seek out child sexual abuse content*, 18 June 2013, available at https://www.gov.uk/government/news/tackling-illegal-images-new-proactive-approach-to-seek-out-child-sexual-abuse-content (12.11.2015).

135 IWF, *A Human Rights Audit of the Internet Watch Foundation*, by Lord MacDonald of River Glaven QC, 2014, available at https://www.iwf.org.uk/assets/media/accountability/Human_Rights_Audit_web.pdf (12.11.2015) , para. 8.3. See section 5 of this country report for more detail.

136 See section 2.1.1. above of this country report for further information.

2003.[137] The IWF's ***URL List Policies, Procedures and Processes***[138] sets out the factors[139] to be considered when imagery is being assessed, as well as the risks potentially associated with adding a URL to the IWF *URL List*, such as whether it will create significant problems for internet users or is likely to lead to increased availability of the image.

5. Assessment as to the case law of the European Court of Human Rights

In light of the limited number of specific legislative provisions governing the blocking, filtering and take-down of internet content, it is true to say that such decision-making is largely left in the hands of internet service providers ("ISPs") themselves. Potentially **unlawful material is often removed in accordance with *Community Standards* or *Acceptable Terms of Use* policies of ISPs**, many of which tend not to tolerate any content which is offensive, abusive or indecent, or which promotes or encourages illegal or socially unacceptable or irresponsible behaviour. The threshold for the kind of material which may be subjected to removal is therefore much lower than that which might otherwise be prescribed by law.

Being conducted by private entities with no particular obligation to respect fundamental human rights, there is less accountability associated with such **"censorship" by ISPs** than would be the case if it was carried out by public authorities, or prescribed by legislative rules. Moreover, the existing legal framework arguably provides strong incentives for ISPs to take down such material without properly investigating complaints. Certainly, in the **absence of domestic laws on notice and take down** (save for a few exceptions), the over-arching framework of the EU's Electronic Commerce Directive as implemented by the UK's Electronic Commerce (EC Directive) Regulations 2002, is claimed to provide ISPs with valuable exemptions from both criminal and civil liability where they act expeditiously to disable access to offending content, particularly where it can be said that they act as hosts of the material in question.[140] As one commentator notes in relation to social networking and search engine sites:

> "The difficulty with such self-regulatory measures is that it leaves the private body to decide what standards apply and make a determination about the content. If the social network or search engine is very responsive to complaints, that may provoke criticisms that it gives too little protection to expression and potentially takes down harmless and lawful material simply because someone objects to it."[141]

Even where statutory rules do exist with respect to notice and take-down procedures (namely, the Terrorism Act 2006 and the Defamation (Operators of Websites) Regulations 2013), the provisions

---

137 Sentencing Council, *Sexual Offences – Definitive Guideline*, available at http://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Definitive_Guideline_content_web1.pdf (09.04.2015).

138 IWF, *URL List Policies, Procedures and Processes*, available at https://www.iwf.org.uk/assets/media/members/URL%20List%20policies%20procedures%20and%20processes%20FINAL%202.pdf (09.04.2015).

139 These are: previously unseen imagery, history and how widely the imagery is disseminated, nature of the imagery, nature of the website featuring the imagery, volume of imagery associated with the URL, jurisdictional legal disparity.

140 See conclusions of C. Ahlert, C. Marsden, C. Yung, *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, (undated), *op. cit.*, p. 27; and analysis of Daithi Mac Sitigh in *The fragmentation of intermediary liability in the UK, op. cit.*, where, for example, he comments that for website hosts, there is, "*inescapable bias in favour of action on the part of the host.*" (p.525).

141 J. Rowbottom, *To rant, vent and converse: protecting low level digital speech*, 2012, The Cambridge Law Journal, 71, pp. 355-383, at p.380.

are not so concerned with safeguards for the protection of freedom of expression, as with offering an exemption from liability for ISPs which follow the relevant process. The manner in which the recent Defamation Regulations will be applied in practice remains to be seen, but with regard to the Terrorism Act, as reported above,[142] it has never been necessary for authorities to rely on the statutory notice and take-down procedures: **ISPs have always cooperated willingly with informal requests to remove offending material**. Accordingly, there is no apparent scope for any meaningful assessment, by those demanding or executing the blocking, of requirements such as necessity or proportionality.

Insofar as blocking mechanisms and the consequences for freedom of speech are concerned, academic commentary and judicial scrutiny in the UK has principally focused on two areas: first, **injunctions issued by the High Court** in connection with copyright and trademark infringement, and secondly, the **activities of the Internet Watch Foundation** ("IWF"). These are addressed, in turn, below.

Injunctions awarded under section 97A of the Copyright, Designs and Patents Act 1988 ("CDPA 1988") requiring ISPs to block or impede access by their customers to peer to peer ("P2P") websites may prevent not only illegal activity, but also may prevent individuals from engaging in lawful activity. In relation to the notorious website, *Pirate Bay*, for example, it has been noted that much of its content is not unlawful, including the promotion of independent musicians and the distribution of free and open source software.[143]

That **such injunctions may result in over-blocking** and a breach of the Article 10 right of freedom of expression is compounded by the argument that **they are restrictions not "*prescribed by law*"**. These arguments were examined carefully by Mr Justice Arnold in the High Court in the *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc*[144] case. Here, he noted that the court had already engaged in a rights balancing exercise, namely the **balancing of the copyright holders' rights under Article 1 of the First Protocol** (acknowledging that these are "rights of others" within Article 10(2)), **with the right to free expression under Article 10(1)**.[145] As to copyright, it was remarked, such balance is primarily struck by the various exceptions and limitations contained in the CDPA 1988.[146] Moreover, with reference to the **ECHR case of *KU v Finland***,[147] it was confirmed that just because the outcome of the balancing exercise may involve an interference with the use of the internet, this does not in itself give rise to any special considerations.

In finding that section 97A orders of the kind adopted in this, and subsequent cases, in which such an injunction is sought are indeed "*prescribed by law*", Mr Justice Arnold made a specific distinction with the blocking order issued against a Belgian ISP which had been considered in the European Court of Justice ("ECJ") case, ***Scarlet Extended SA v SABAM***.[148] In that case, the ECJ had ruled that an injunction made against an ISP which required it to install a wide-ranging filtering system was incompatible with various EU Directives when construed in light of fundamental rights, including Article 10. In contrast, Mr Justice Arnold declared that the High Court here was faced with a request for an **order which was clear and precise**, merely requiring the ISP in question to implement an

142 See section 2.1.2. of this country report above.

143 See Pirate Party UK, *The Pirate Party UK's Proxy for Pirate Bay*, 10 May 2012, press release, as cited in A. Murray, *Information Technology Law*, *op. cit.*, p. 73.

144 *Op. cit.*

145 *Ibid*, para. 164.

146 Namely, Part 1, Chapter III of the CDPA 1988, which sets out the acts which are permitted in relation to copyright works.

147 *KU v Finland* 2872/02 [2008] European Court of Human Rights 1563 (2 December 2008).

148 (C-70/10) [2012] European Copyright and Design Reports 4.

existing and technically feasible technical solution, with provision made for the order to be varied or discharged in the event of a future change of circumstances. Such an order, it was held, would fall, "*well within the range of orders which was foreseeable by ISPs on the basis of section 97A…*" and **was therefore one prescribed by law**.[149] As to proportionality, the Judge was also satisfied that the order sought by the Studios was **proportionate**, being **necessary** and **appropriate to protection Article 1 First Protocol rights of the Studios** and other copyright owners, which he said, clearly outweigh the Article 10 rights of the users of the pirate website (as well as the operators of the website itself).[150]

Featuring the same characteristics as the section 97A order issued in this case, **subsequent injunctions based on similar wording have been able to resist challenge**, and are now regularly awarded on paper without the need for a court hearing.

In the more recent case of *Cartier International AG and Ors v British Sky Broadcasting & Ors,*[151] Mr Justice Arnold re-examined the requirement that any limitation on rights be "*prescribed by law*" in light of the ECHR case of ***Yildirim v Turkey***.[152] In the absence of a specific legal provision (equivalent to section 97A of the CDPA 1988) protecting **internet trademark infringement**, the rights holders sought to rely on section 37(1) of the Senior Courts Act 1981 which provides a general right to the High Court to grant an injunction, "*in all cases in which it appears to be just and convenient to do so*." The ISPs however, referred to the Concurring Opinion of Judge Pinto de Albuquerque in *Yildririm v Turkey* that general provisions governing civil and criminal responsibility do not constitute a valid basis for ordering internet blocking. In confirming that **a blocking injunction under the Senior Courts Act 1981 was one prescribed by law**, Mr Justice Arnold relied on the majority judgment of the Second Section in *Yildirim v Turkey*, which held that to be "*prescribed by law*" means the impugned measure having some basis in domestic law while also referring to the quality of the law: that it should be accessible to the person concerned and compatible with the rule of law.[153]

Accordingly, insofar as copyright and trademark infringement blocking injunctions are concerned, the English courts are satisfied that, where the text of such orders respects the customary format, **there will be no breach of legal principles, including fundamental rights**. This is **reinforced by standard safeguards against abuse**, notably that both the ISPs and operators of the target websites may apply to the court to discharge or vary the orders in the event of any material change of circumstances, and, more recently, that subscribers be informed when accessing blocked websites that they have the right to apply to discharge or vary the order and that such blocking orders should, where appropriate, cease to have effect at the end of a defined period.[154]

The **role and activities of the IWF in blocking child abuse images**, on the other hand, have been criticised as being far less likely to respect the core principles of legitimate interference with the

---

149 *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc* [2011]*, op. cit.* at para. 177.

150 *Ibid*, paras. 199-201.

151 *Op. cit.*

152 Application No. 3111/10, 18 December 2012.

153 It should also be noted that the Court considered the following requirements before granting the orders sought (primarily in light of the EU Directive 2004/48/EC on the enforcement of intellectual property rights ("the Enforcement Directive")), namely that: (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; and (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.

154 See section 2.1.4 of this country report above, in relation to *Cartier International AG and Ors v British Sky Broadcasting & Ors*.

fundamental right of freedom of expression. These, and other issues related to human rights, were examined as part of an independent audit commissioned by the IWF and conducted in 2013 by a former Director of Public Prosecutions. This was published by the IWF in January 2014. Entitled, "***A Human Rights Audit of the Internet Watch Foundation***"[155] (the "IWF Human Rights Audit"), this concluded that the IWF's practices were generally consistent with human rights law, but made a series of recommendations for improvements, the majority of which the IWF has accepted and subsequently acted on. Some conclusions of the report are referred to below.

As to criticisms, it is, firstly, not clear that the IWF is, in any event, subjected to the European Convention on Human Rights. Under section 6 of the UK's Human Rights Act 1998, which gives direct effect to the European Convention under UK domestic law, the Act is said to be only binding on "public authorities". As discussed in section 2.1. above, the **IWF is not a public authority, but a registered charity**. It may nevertheless qualify as a public authority by virtue of its public functions. As one commentator points out, while there is no legislative underpinning to the functioning and legitimacy of the IWF, there can be no question that its legitimacy and role is government driven.[156] This view is supported by the findings of the IWF Human Rights Audit, which states in its Executive Summary that, "*…it is highly likely that IWF's acts would be construed by the Courts as public acts, so that its policies and decision-making are in reality susceptible to judicial review, and may be overturned by the Courts were it ever to be found that the IWF was exercising them in a manner incompatible with human rights law*."[157]

Secondly, if it can be concluded that the IWF can be classified as a public authority by virtue of its public activities, or if it may be said that the State has positive obligations to the public under Article 10 of the ECHR concerning the governance of the IWF, it has also been **questioned whether the IWF and its activities are "*prescribed by law with a legitimate aim*,"** such that it may legitimately limit freedom of expression. Although it certainly has legitimate aims, such as the prevention of crime and the protection of morals and public safety, it is doubtful that its powers of censorship can be said to be prescribed by law. Its administration is not prescribed by law and its **lack of accountability and transparency** leaves its decision making **open to arbitrariness and a lack of accessibility**. As the *Open Rights Group* points out, "*the legality of the materials added to the IWF's blacklist has never been assessed by a court or other qualified and accountable legal body, and there is nothing stopping legal material being included on the list, neither inadvertently nor deliberately*."[158]

For its part, the IWF stresses that with regard to **transparency**, as a registered charity, its accounts are audited and published, alongside other policies and appeals processes, including on "splash" pages which are displayed when users attempt to access a blocked web page.

Some of the criticisms aimed at the IWF's perceived lack of accountability are also explored in the IWF Human Rights Audit. Acknowledging that the work of the IWF is of a public nature and would

---

155 Available at https://www.iwf.org.uk/assets/media/accountability/Human_Rights_Audit_web.pdf (11.11.2015).

156 E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation*, *op. cit.,* p. 324. This view is supported by the findings of the Human Rights Audit, which states in its Executive Summary that, "*…it is highly likely that IWF's acts would be construed by the Courts as public acts, so that its policies and decision-making are in reality susceptible to judicial review, and may be overturned by the Courts were it ever to be found that the IWF was exercising them in a manner incompatible with human rights law*."

157 The IWF Human Rights Audit, *op. cit.*, p.5

158 Open Rights Group web pages, *Internet Watch Foundation*, available at https://wiki.openrightsgroup.org/wiki/Internet_Watch_Foundation (15.04.2015).

almost certainly be susceptible to challenge on human rights grounds,[159] the Audit's author goes on to examine how regulation of the internet by such a private body can comply with human rights principles. To have some sort of **judicial authorisation prior to blocking or takedown notices being issued, the author concludes, would be unworkable** in light of the sheer number of reports of illegal content, and would threaten the efficiency and speed of removal which the system demands.[160] Such judicial scrutiny, says the author, would be an inevitable corollary of the alternative to the member-ship-based voluntary process run by the IWF, namely a government-run system operated by a police body.[161] **Judicial review, in the opinion of the author, provides an appropriate and sufficient mechanism** for providing reassurance that the IEF's work remains consistent with human rights principles. Nevertheless, the author recommended that the accountability of the IWF's appeal process for challenging the assessment of content be reinforced with a final layer of appeal to be overseen by a retired judge.[162] Additionally, it was recommended that an **expert in human rights law be appointed to the IWF's Board** and that a **senior legal figure be appointed as new Chief Inspector**, with responsibility for conducting independent inspections of IWF's work at least every two years.[163] It is understood that these recommendations were subsequently accepted by the IWF Board.

Thirdly, it has been questioned whether the IWF's interference with the right to freedom of expression is **necessary and proportionate**. The blacklist operated by the IWF effectively amounts to censorship, removing from public access the webpages concerned. The extent to which this method is "*necessary in a democratic society*" is difficult to assess, because it is not clear what material is being censored.[164] Not only are the blacklist and notices sent to members of the IWF kept secret, but there is no requirement to notify website owners when their site has been added to the blacklist.[165] In its defence, the IWF emphasises that the webpages included on its blacklist are at the **most specific level possible (*URL*s)** and that the list itself is **updated twice per day** to reduce the possibility of over-blocking. It is also reported that the **IWF describes the blacklist as voluntary**, whereby ISPs choose to remove access to offending sites.[166] However, in practice, in light of their obligations under the *Code of Practice* of the UK's Internet Service Providers Trade Association, the ISPA, it may be said that **members have little alternative** but to remove content which is notified to them as being illegal.[167]

Addressing some of these criticisms, the author of the IWF Human Rights Audit points out that the **blocking list is, for obvious reasons, not published more widely** and that complaints of critics that

---

159 IWF Human Rights Audit, *op. cit.*, para 7.8.

160 *Ibid*, paras. 6.3-6.4 and 7.7.

161 "*I consider that there would be great reluctance simply to empower police to issue notices in circumstances where the law required those notices be strictly complied with on pain of penal sanction in the absence of judicial endorsement of any sort…"* (IWF Human Rights Audit, para. 5.1.15).

162 This recommendation has since been adopted by the IWF, and former High Court Judge, Sir Mark Hedley, currently holds the positions of appeals commissioner and chief inspector. See IWF webpage, *Human Rights Audit*, available at https://www.iwf.org.uk/accountability/human-rights-audit (11.11.2015).

163 IWF Human Rights Audit, paras. 4.2., 5.2.10 and 5.3.3.

164 See A. Murray, *Information Technology Law, op. cit.,* p. 382.

165 See also Wolfgang Benedek and Matthias C. Kettemann, *Freedom of Expression and the Internet*, Council of Europe Publishing, 2014, which refers to criticisms of the IWF, "*…including non-illegal websites in its blacklist with immediate negative effects for website owners and Internet users, without any notice of blocking or review procedure (or even a judicial assessment of legality) that would be consistent with human rights.*"

166 E. B. Laidlaw, *The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation*, *op. cit.*, p. 329.

167 See 2.1.1. of this country report above; the ISPA is the UK's Trade Association for providers of internet services.

the process is thereby rendered unacceptably opaque are, in his opinion, unreasonable.[168] In light of the criminal nature of the content which fall within the IWF's remit, restrictions are, according to the author, **self-evidently "prescribed by law"**. Restrictions on **child sexual abuse content** in particular, which accounts for more than 99% of the content dealt with by the IWF, are, in the view of the author, **a proportionate interference in privacy and free expression, necessary to protect vulnerable children from exploitation and grave abuse**. Moreover, the identification of child sexual abuse content is relatively straightforward and the risk of misidentification minimised, even where prior judicial authorisation is not sought. Unlike child sexual abuse content, however, the **assessment of the unlawfulness of adult pornographic content[169] is a sensitive area** which presents special difficulties for a private body exercising judgments in areas which are very likely to engage ECHR privacy and free expression rights, and which demand legal expertise.[170] In the absence of in-house legal specialists, the IWF, he concludes, is probably not best placed to engage in such policing. A recommendation that the IWF in future restrict its remit only to child sexual abuse material is currently being considered by the IWF.[171]

John Curran, LL.M.
Researcher at the SICL
October 2015

Revised on 03.05.2016 taking into consideration comments from the United Kingdom on this report

168 IWF, Human Rights Audit, para. 1.7.

169 Almost none of which, in 2014, was hosted with the UK, and therefore did not fall within the IWF's remit (IWF, *Annual Report 2014, op. cit.,* p. 16.).

170 IWF, Human Rights Audit, para. 3.9.

171 In order to better ensure compatibility with international human rights obligations, the author also recommended that analysts involved in proactive investigations, subsequently introduced in 2014, be provided with specialist training in the law and in investigative techniques, and that they liaise closely with the police. The IWF reports that these recommendations were subsequently accepted (IWF web page, *Human Rights Audit*, *op. cit.*).