EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online

Policy Analysis for the European Financial Coalition

Possible implications for web hosting companies of using image recognition technology to detect known child abuse material uploaded by users to their network

Professor Ian Walden and Tim Crosland*

* The authors would like to thank the following individuals for their valuable help in the preparation of this report: Giovanni Maria Riccio, John Carr, Fred Langford, Andy Morling, Robyn and Greeves Edward Gbajumo. The views, however, are solely the authors'.

This project has been funded with the support of the European Commission. This publication reflects the views only of the author. The European Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

1. Introduction

The European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC) is a project funded by the ISEC Programme of the European Commission. It brings together key actors from law enforcement, the private sector and civil society in Europe with the common goal of fighting the commercial sexual exploitation of children online. Members of the EFC join forces to take action on the payment and ICT systems that facilitate such crimes.

Between 2009 and 2010 EFC undertook a project to combat commercial websites supporting the trade in child abuse material, helping to reduce their number. New challenges were being identified, however, including the migration of material from traditional commercial websites towards other new and existing Internet environments and platforms, in response to which EFC launched its 'second phase' in November 2012.

Current EFC activities are divided into 5 'Work Packages'. Work Package 3 focuses on private sector support and cooperation. This report aims to fulfill part of this mandate, and specifically:

> **To conduct a policy analysis on the possible implications related to the use of such image recognition technology by web hosting companies to detect known child abuse material uploaded by users to their network.**

The report considers in particular the intent and implications of the 'E-Commerce Directive' (ECD)[1], specifically Article 14, which limits the potential liability for hosting providers in relation to illegal content; and Article 15, which prevents states imposing on intermediary service providers (including host providers) any general obligation to monitor the information they transmit or store. These provisions have sometimes been viewed as a reason for inaction by web hosting companies against illegal content stored on their service, including child sexual abuse images, on the grounds that 'doing nothing' shields them from liability. Indeed, with regard to monitoring, the provisions have sometimes been characterized as an obligation on intermediaries, rather than a constraint on Member States. This report examines the veracity of these positions and considers the complex set of legal risks that attach to both the taking of action against child sexual images, as well as the temptation towards inaction. In this respect, the deployment of IRTs can be viewed as simply one option for action, a case study.

However it is not possible to properly assess the policy implications of using IRTs without extending the scope of the analysis into other areas of law, including data protection and human rights. Critically the report does not confine itself to an analysis of the risks of using IRTs; it

[1] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178/1, 17.2.2000)('ECD').

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

also considers the risks of *not* doing so, including the risks of allowing child abuse images to be re-uploaded once taken offline, so-called 'stay-down'. Only by considering both sides of the argument can appropriate policy recommendations be made.

This report is not intended as legal advice regarding the position in any one or more EU Member State. Rather, by presenting an overview of the broader legislative and jurisprudential trends across the EU, it is designed to assist hosting companies in taking an informed decision on whether the use of IRTs would be appropriate.

There is a need for one further caveat. The conclusions, which follow, are context dependent. Although ECD does not distinguish between types of illegal content, it is clear that the courts do. As a class, images of child sexual abuse are an obvious example of 'manifest illegality', and their removal does not usually involve complex balancing exercises with competing interests such as freedom of expression[2]. Consequently, it is not being argued, nor should it be assumed, that the same or similar conclusions would apply to the use of similar technologies in other contexts.

2. IRT Technologies[3]

While this report focuses on the policy implications of the deployment of IRTs, rather than the technology itself, it is important to consider whether the mode of IRT deployment can impact on the legal analysis and therefore the available policy options.

In simplistic terms, all IRTs can be said to comprise two key elements:

- A database of reference images or unique IDs[4] of child abuse material[5], against which the solutions scan; and
- A mechanism by which the target material is scanned, whether it is held in storage capacity (e.g. a hard drive), network streams (i.e. on upload) or crawling the web for URLs (i.e. on download).

From a legal perspective, where the database contains actual images, rather than some unique reference ID, then possession of the database itself would constitute a criminal offence, in the

[2] However, see further section 3 below.
[3] See EFC 'Overview of Image Recognition Technologies for Internet Service Providers for the prevention and protection of their services from misuse related to commercial sexual exploitation of children online.' ('EFC Overview'). The report's authors would also like to acknowledge the assistance of Fred Langford, Director of Global Operations, Internet Watch Foundation on this section.
[4] The use of unique IDs improves the efficiency of the processing, in terms of volume and speed, as well as avoiding the need for further distribution of the illegal content.
[5] E.g. photographs or videos. The database could be limited to victim identification or include other relevant material, e.g. shape of window, which could enable scene identification.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

absence of specific legal immunity or defence. As a consequence, IRTs deployed by the private sector will utilize unique IDs.

The unique ID or 'fingerprint' may be created using either cryptographic or perceptual hashing techniques[6]. An advantage of the former is the process can be completely automated, without the need for human review, since the matched image will have a 100% correlation. So, for example, a web-host can action the match (e.g. report it to an appropriate body) with little, if any, risk of a false positive and no need for human review. Perceptual techniques involve taking reference points from the image, which enables different match tolerances to be set in order to be able to capture images that have been altered or manipulated (e.g. cropped, stretched or rotated), whether deliberately or otherwise. However, the looser the tolerance for matching, the greater the likelihood of false positives being identified, generating the need for human review and the associated legal risks depending on what action is taken.

In terms of the scanning process, IRTs operate primarily by analyzing the content of the hosted material, rather than any meta-data associated with that content[7]. As a consequence, the conduct of scanning could be construed as a form of illegal interception (see further at 5.1 below)[8]. As such, the web-host provider will want assurance that it will either be able to rely on a statutory defence or that it will not be subject to criminal proceedings.

Finally, for the purposes of this report, the authors have presumed that the terms of service ('ToS') of web-host providers expressly refer to deployment of IRTs for the purpose of detecting child sexual abuse materials and how they operate (in broad terms), i.e. the deployment of such techniques is not kept secret from service users. In addition, any acceptable use policy ('AUP') applicable to provision of a web-host service expressly prohibits the use of the service for storing illegal conduct. Such transparency and private law provision will be important in terms of managing the legal risks.

3. Child sexual abuse images

Further to the discussion of the technology, it is also necessary to consider the legal nature of the images themselves. As noted, above, child sexual abuse images are widely recognized as 'manifestly illegal'. However, the legal reality is more complex. The following are examples of situations where a hosted image may not be considered illegal:

1. Under EU law, 'child pornography' is defined as including material of a "person

[6] E.g. MD5 and Microsoft's PhotoDNA respectively.
[7] Given the range of different systems on which, and through which, an image will have been processed during its lifecycle, such meta-data is likely to be highly misleading.
[8] See further 5.1 below.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

appearing to be a child"[9]. However, Member States have the option of not criminalizing such material where the person is in fact over 18 years of age.

2. While a 'child' is defined as under 18 years of age, the law of some Member States recognize that the making of images relating to persons over the 'age of sexual consent'[10] but under 18 may be permitted where the person is in an appropriate relationship with another person[11].

3. EU law allows Member States not to criminalize the possession of 'realistic images', where it does not involve real persons and such possession does not involve risk of dissemination[12].

Together, these examples illustrate that although EU criminal law has been harmonized, some divergences remain. Broadening the perspective to the international realm, the legal situation inevitably becomes even more varied and complex. As a consequence, while an image may be considered illegal in one state, e.g. the 'hosting state', it may not be illegal in another, e.g. the customer's state. Such disparities in law are unlikely to be coded for in the operation of IRTs, therefore raising the possibility that legal images may be incorrectly identified when scanning hosted content, i.e. false positives.

A second area of legal complexity can arise when use of an image engages issues of conflicting rights, particularly freedom of expression, which may require some form of balancing exercise to be carried out when removing such material. While child sexual abuse images are generally recognized as a "specific type of content which cannot be construed as the expression of an opinion"[13]; given the blurred boundaries noted above about what constitutes an illegal image, examples of conflicting rights can arise. In December 2008, the Internet Watch Foundation decided to place on a block list an image of a naked prepubescent girl from the album cover of *Virgin Killers* by the band the Scorpions; considering it to be potentially illegal. The image was part of a page on Wikipedia that discussed the controversy surrounding the image. As a result of the block, both the image and associated text were rendered inaccessible, while other users of the Wikipedia site were also prevented from editing entries on Wikipedia. In another example, the European Court of Human Rights was asked to consider whether the expression rights of a Finnish artist had been unlawfully interfered with by her prosecution for the possession and public display of child sexual abuse images, against her stated aim "to encourage discussion and raise awareness of how wide-spread and easily accessible child

[9] Directive 2011/92/EU 'on combating the sexual abuse and sexual exploitation of children and child pornography' (OJ L 335/1, 17.12.2011)('Child Protection Directive'), at art. 2(c)(iii).
[10] Ibid., at art. 2(b): "means the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child". In the UK, for example, this is 16.
[11] E.g. UK: Protection of Children Act 1978, s. 1A, e.g. 'sexting'. Such a scenario is also provided for in Council Framework Decision 2004/68/JHA 'on combating the sexual exploitation of children and child pornography', at art. 3(2)(b); although since repealed.
[12] Child Protection Directive, at art. 5(8). In the US, the Supreme Court considered similar such legislative provisions as overbroad and therefore potentially unconstitutional; see Ashcroft v Free Speech Coalition 535 US 234, 244 (2002).
[13] Child Protection Directive, at Recital 46.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

pornography was"[14]. In these cases, the legitimate expression rights of individuals may need to be given adequate consideration when determining the legality of an image and making a determination to either block or remove it.

In both scenarios, regarding the legality of an image or the context of its use, such complexities could have implications for the deployment of IRTs. On the assumption that IRTs cannot be coded to take into account such legal subtleties, such issues have to be addressed either when assembling the database of reference images or unique IDs the IRT uses, or post-identification, by the person responsible for taking action on a report; or indeed at both stages.

Although it is important to be aware of differences in the definition of 'child sexual abuse images', the issue ought not to be exaggerated or be an excuse for inaction. The volume of abuse images in circulation drives law enforcement and others to focus on the 'worst-of-the worst'. Centralized databases, on which IRTs depend, will generally only include those that are 'manifestly illegal', images that reside well within the legal boundaries of any jurisdiction that criminalizes such images, e.g. young children (under 12) and classified as being of a particular level of seriousness[15]; or by altering the threshold for matched images detected by the system's algorithm[16]. In practical terms, therefore, definitional differences between jurisdictions should not be a reason for inaction.

From a liability perspective, the hosting company will want to be able to place reliance on either the pre- or post-scanning process to limit its exposure to any claim from a customer resulting from a false positive identification. Our recommendations regarding the availability of competent authorities to take coordinated and consistent action in relation to identified images (see section 7 below) aim at narrowly circumscribing the role of companies (and therefore their potential liability for action taken).

[14] Application No. 1685/10, Karttunen v Finland (2011). The Court held that the claim was inadmissible, in part because the domestic court had "balanced at length" the conflicting interests (para. 24). One can speculate whether the result would have been the same had the images not involved real children, but rather 'realistic images'.
[15] There are various categorization schemes for such images, such as the COPINE scale. See Taylor, M., G. Holland and E. Quayle, "Typology of paedophile picture collections", 74 Police Journal 97 (2001). In the UK, images are categorized on a scale from A-C (Sentencing Council, Definitive Guideline, 2013), where A is the most serious; so the database may be limited to those images only.
[16] See EFC Overview.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

4. Intermediary Liability for 'Hosting'

The Internet, for all its social and economic benefits, itself presents substantial challenges to the rule of law: partly because it transcends traditional jurisdictional boundaries; and partly because it blurs the distinctions between public and private functions and responsibilities. As human activity is conducted increasingly through the online environment, Internet intermediaries are seen by some as the front line in the fight against crime and terrorism.

Any requirement that intermediary companies should proactively 'police' illegal content, however, gives rise to four broad sets of concerns:

1. It may expose the intermediary to liability for any illegal content they locate being 'hosted' on their service;

2. It will result in controls being placed on service usage that impede free expression and the flow of information, such a feature of the online environment;

3. It may impose on intermediaries a substantial cost burden, potentially stifling innovation and growth; and

4. Intermediaries, as private actors, are seen as lacking the mandate and competence to undertake what can often be a complex balancing exercise, in which considerations of crime prevention and national security lock horns with those of privacy and free speech.

This report is concerned with the first of these concerns, the risk of liability. It is also limited to one specific role of an intermediary in an Internet environment, the provision of resources on which third party data can be stored. European Union law contains provisions shielding intermediaries that 'host' data from the risk of liability related to such data. The key provisions are contained in the Electronic Commerce Directive.

4.1 The Electronic Commerce Directive

The ECD attempts to balance the competing policy considerations, providing a skeleton framework for intermediary liability. The four articles in Section 4 of the ECD were adopted after considerable debate amongst, and lobbying of, the Community institutions. Section 4 of ECD addresses the 'liability of intermediary service providers' engaged in three forms of conduct: 'Mere conduit' (Article 12); 'Caching' (Article 13) and 'Hosting' (Article 14). The fourth article, 'No general obligation to monitor' (Article 15), prohibits Member States from imposing 'general'

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

monitoring obligations on the intermediaries.

'Mere conduit' services are akin to traditional conveyance services, but are a minor component of a provider's overall service offering[17], although they will involve storage elements[18]. 'Caching' is used as a means to limit the need for the retransmission of information from the point of origin, therefore reducing network congestion and improving information provision[19]. For the purposes of this report, however, we are concerned with the 'hosting' shield.

Article 14 states that providers should be protected from liability where:

> **the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent[20].**

Notable are the different conditions established for liability generally and liability for 'claims for damages'. Although the distinction is generally taken to be that between criminal and civil liability, the Article itself does not express it in those terms and it has not been uniformly implemented.

If the provider does have the requisite knowledge or awareness then the protection will only apply on condition that:

> **upon obtaining such knowledge or awareness, [it] acts expeditiously to remove or to disable access to the information.**

Article 15, states that there shall be 'no general obligation to monitor', while providing that obligations may be imposed on providers to provide information regarding 'alleged illegal activities'.

A number of recital provisions assist in the interpretation of Section 4 and Article 14 in particular. Recital 40, for example, reveals that ECD was not intended to create a disincentive to voluntary co-operation to remove and disable access to illegal information:

> **service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for**

[17] See further section 4.1.1.
[18] ECD, at art. 12(2).
[19] Ibid., at art. 13(1).
[20] Ibid., at art. 14(1)(a).

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

> **removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.**

Recital 42 explains that the exemptions from liability apply only to companies providing services of a technical or automatic nature:

> **(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.**

Recital 45 explains that the exemptions do not preclude injunctions requiring the removal of illegal information[21].

Recital 46 makes two significant points regarding the process for removing or disabling access to illegal information once the provider has become aware of it: first the process needs to observe the principle of freedom of expression (not a substantial consideration in the context of images of child abuse); second it should be conducted in accordance with procedures established at national level:

> **(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of**

[21] See Section 4.1.5 below.

> **expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.**

Recital 48 states that the ECD does not prejudice any provisions imposing on service providers duties of care to detect and prevent certain types of crime[22].

Recital 60, urges a legal framework that is:

> **… clear and simple, predictable and consistent with the rules applicable at international level …**

Finally Recital 10, states that the ECD should ensure a high level of protection of objectives of general interest, in particular the protection of minors.

Chapter III of the ECD, deals with implementation. Article 16 encourages the development of codes of conduct, and specifically:

> **… the drawing up of codes of conduct regarding the protection of minors and human dignity[23].**

Having outlined the relevant provisions and accompanying recitals, the following sections examine the various components of Articles 14 and 15 in greater depth. Specifically, we consider the risks of relying on these provisions to justify inaction against images of child sexual abuse.

4.1.1 Web hosting as an 'information society service'

The overarching objective of ECD is to improve the functioning of the internal market in the provision of 'information society services' ('ISS'), defined in accordance with Directive 98/34/EC[24] as:

> **"any service normally provided for remuneration, at a distance, by electronic**

[22] See Section 4.1.6 below.
[23] ECD Art. 16(1)(e). See also Recital 49: "Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes."
[24] Directive 98/34/EC 'laying down a procedure for the provision of information in the field of technical standards and regulations' (OJ L 204/37, 21.7.1998); as amended by Directive 98/48/EC (OJ 217/18, 5.8.1998), at Art 1(2).

means and at the individual request of a recipient of services".

The scope and application of this definition is obviously critical, since other types of service providers will not be able to rely on the immunity provisions, particularly article 14.

Radio and television broadcasting services are excluded from the application of the Directive, as well as 'telecommunication services'[25]. Both categories of service are excluded because other EU harmonizing legislation regulates them. 'Television broadcasting' is a form of 'audio-visual media service', which also includes 'on-demand audiovisual media services'. While the former is not an ISS, the latter are considered being for the purposes of the notification obligation[26]; although the exercise of 'editorial responsibility' that characterizes 'on-demand' service providers effectively prevents them from relying on the 'hosting' defence under Article 14 of the ECD.

In the field of telecommunications, the provision of 'electronic communication services' ('ECS') is defined in the following terms:

> **'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks[27];'**

The boundary between these two types of services, ISS and ECS, would seem particularly blurred, given the variety of approaches that could be adopted for interpreting the phrase '*mainly* in the conveyance of signals'; from quantitative to qualitative measures, including the imputed intention or effect of suppliers in the market and the perception of consumers[28]. So, for example, how should a provider of broadband internet access that offers its customers 5GB of cloud storage as part of a package[29], be characterized from a regulatory perspective? If an ISS, then it will be able to rely on Article 14 of the ECD. If the service is considered an ECS, then

[25] Ibid., at Art. 1(5).
[26] Directive 2010/13/EU 'on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services' (OJ L 95/1, 15.4.2010), at Recital 17.
[27] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (OJ L 108/33, 24.4.2002), at Art. 2(c).
[28] See Walden, I., 'European Union Communications Law', at 4.2, in Walden (ed.), Telecommunications Law and Regulation, 4th ed., Oxford University Press, 2012.
[29] E.g. BT's Infinity fibre broadband and phone package, available at: http://www.productsandservices.bt.com/products/broadband-packages/

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

the issue of its liability for any illegal content stored on the service will need to be determined under domestic legal principles as well as EU law, since the European regime does not fully address such matters.

Under the Communications Privacy Directive[30], providers of ECS are prohibited from the interception and surveillance of communications and related traffic data, except where legally authorized to do so[31]. This prohibition is an analogue of the obligation not to monitor provision at Article 15 of the ECD. However, while it is applicable to its transmission service and any 'technical storage which is necessary for the conveyance of a communication', it does not offer ECS providers immunity in respect of any associated 'hosting' services akin to that under Article 14. As such, an ECS provider would need to rely on any domestic law provisions or principles that offer similar protections[32].

The role of legal consistency and certainty in supporting the internal market in information society services and consumer confidence is emphasized in the ECD. However, as evident from the discussion above regarding the definition of ISS, and as will become further apparent, it is questionable how far ECD has succeeded on this score concerning the liability of Internet intermediaries[33].

4.1.2 What constitutes 'hosting'?

Exemption for liability under the ECD Article 14 depends on the provider being able to demonstrate that the relevant activity constitutes 'hosting'. Legal uncertainty concerning this term means that even before consideration of the limits of the exemption, consideration should be given as to whether it applies in the first place.

In the case of *L'Oreal SA v eBay International AG*[34] the Court of Justice of the European Union, in considering the question of 'whether the service provided by the operator of an online marketplace is covered by Article 14(1) of Directive 2000/31', emphasised that the applicability of the provision would vary with context. L'Oréal had brought proceedings against eBay and a number of its users in various European countries, including in the English High Court, on the basis that they were not taking sufficient steps to stop the sale of counterfeit and other trademark infringing goods.

The Court noted firstly that an internet market-place (i.e. 'an internet service consisting in

[30] Directive 02/58/EC 'concerning the processing of personal data and the protection of privacy in the electronic communications sector' (OJ L 201/37, 31.7.2002).
[31] Ibid., at art. 5(1).
[32] E.g. a requirement to evidence 'knowledge'.
[33] See EDiMA, Towards a workable and balanced environment for online intermediaries.
[34] Case C-324/09, L'Oréal SA & ors v eBay International AG & ors [2012] E.M.L.R. 6.

facilitating relations between sellers and buyers of goods') falls within the scope of the ECD as an information society service; and that it was not disputed that eBay stores in its server's memory data supplied by its customers. However the Court held that:

> **… the fact that the service provided by the operator of an online marketplace includes the storage of information transmitted to it by its customer-sellers is not in itself sufficient ground for concluding that that service falls, in all situations, within the scope of Article 14(1) … That provision must, in fact, be interpreted in the light not only of its wording but also of the context in which it occurs and the objectives pursued by the rules of which it is part[35].**

More specifically the Court held that:

> **Where … the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1)[36].**

Although the test of neutrality appears reasonably clear-cut, different approaches have been taken in different national courts. Whereas judgements from Germany[37] and Austria have tended to support the status of auction platforms as host providers, the Dutch courts appear to have taken a more nuanced approach[38].

Member states have likewise adopted different approaches in relation to other specific forms of service. The ECD, for example, does not contain provisions regulating information location tools, such as search engines, but it contains a provision calling upon the Commission for a period of re-examination every two years, which includes in particular "the need for proposals concerning the liability of providers of hyperlinks and location tool services"[39]. Some states,

[35] para. 111.
[36] para. 116.
[37] BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I.
[38] District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031/HA ZA 05-211; see also Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211.
[39] Article 21(2). No such change has been proposed.
[40] Federal Act on Certain Legal Aspects of Electronic Commerce and Legal Transactions [2001] Bundesgesetzblatt (Österreich) I 1977 (21 December 2001), at s. 14 (search engines) and 17 (links).
[41] Act CVIII of 2001 on certain aspects of electronic commerce services related to the information society, at art.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

however, have adopted specific legislation in this regard. Austria, for example, has introduced a liability exemption for search engines that mirrors ECD Art 13 (relating to access providers)[40]; whereas the Hungarian legislation treats them as host providers[41]. In France there is no specific legal regime, but the courts have sometimes found a search engine to fall within the definition of a host provider[42]. They have also held that search engines must filter the contents of their automated indexes for illegal content such as racist material[43]. In Germany, in a case dealing with trademark infringements, the court held that a search engine might be found liable as an accessory only where the infringement was gross and obvious, or had been directly notified[44]. In Belgium the Supreme Court ruled that the owner of a website containing hyperlinks referring to child abuse images could not benefit from a host provider's liability privilege[45]. It appears, however, that this was on the basis that the owner had knowledge and control of the content.

Amid such variation and uncertainty it may be unwise for a company to assume the protection of ECD Article 14 in relation to all of its services across the EU.

4.1.3 Knowledge, awareness and control

Where a person hosts content on behalf of another, two related questions arise: Does the person have knowledge of the content? Does the person exercise control over it? First, the person may become aware of the nature of the content being held, whether illegal in itself, such as child abuse images, or as evidence of illegal behaviour. Second, with that knowledge, the possibility exists that the content can be removed or acted upon in some other manner and, or, passed on to the appropriate authorities, in cases of criminality, or others, where such material causes harm capable of giving rise to civil suit. Knowledge may be a sufficient condition to attract liability (where, for example, there is an obligation to report)[46]; while control may confer responsibilities and obligations upon an intermediary to act, such as preventing the uploading of illegal material[47]. Critically, knowledge is a necessary pre-requisite to the exercise of control, whether the control is carried out proactively or reactively. Proactive monitoring for particular content requires knowledge of the content being sought, while reactive removal of content requires knowledge of its existence.

The liability shield is only applicable up to the point at which the web-host obtains 'knowledge or awareness'. What comprises such knowledge and awareness is obviously a fact to be determined in the particular circumstances. Article 14(1)(a) refers to 'actual knowledge', which may

[42] Comm Lille, 01/06/2006, STE Espace Unicis c/ SA Meetic, SARL Google France www.juriscom.net/documents/tclille20060601.pdf.
[43] TGI Paris, 11/02/2003, UEJF et Licra c/ Yahoo! Inc. et Yahoo France
[44] LG Hamburg, 21/9/2004, 312 O 324/04, MMR 2005, 631
[45] Cour de cassation, 3 févr. 2004, R.D.T.I., 2004, n° 19 ; En première et seconde instance : Tribunal pp. 166 et s
[46] Conduct giving rise to strict liability is not considered in this report.
[47] E.g. in March 2012, a German court ordered RapidShare to block the uploading of some 4000 files known to contain infringing copyright material. See https://edri.org/edrigramnumber10-6german-court-filtering-rapidshare/
[48] Electronic Commerce (EC Directive) Regulations 2002, at r. 22. In CG v Facebook [2015] NIQB 11, the judge considered actual and constructive knowledge as synonymous in the context of Article 14 (at para. 94).

be considered synonymous with, or distinguishable from, other forms of knowledge such as constructive knowledge or 'wilful blindness'. In the UK, the implementing regulation adopts an all encompassing approach, requiring a court to "take into account all matters which appear to it in the particular circumstances to be relevant"[48]. 'Awareness' is a lower standard, which reflects the distinction between criminal and civil liability, the former requiring the higher threshold.

The majority of member states (Austria, Belgium, Cyprus, Denmark, Estonia, France, Germany, Greece, Ireland, Italy, Lithuania, Luxembourg, Portugal, Slovenia, Sweden, UK) have carried out near verbatim transpositions of Art 14 into their national legal systems. Some member states have slightly modified the wording of the directive. The Dutch implementing legislation states that a provider 'cannot reasonably be expected to know of the illegal nature of an activity or information' (Art 6:196c (4) Civil Code). The Portuguese law (16 Law-Decree No. 7/2004 of 7 January 2004) states that civil liability 'shall still remain whenever, relating to known circumstances, the service provider should be aware of the illegal character of the information.' If such approaches come close to establishing a due diligence requirement, they should not be regarded as atypical. Indeed in interpreting Art 14(1)(a) the ECJ, in *L'Oreal SA v eBay International AG*, adopted a similar formulation, stating:

> **it is sufficient, in order for the provider of an information society service to be denied entitlement to the exemption from liability provided in Article 14 … for it to have been aware of facts or circumstances on the basis of which a *diligent economic operator should have identified the illegality in question*[49]** [emphasis added] **… Moreover, if the rules set out in Article 14(1)(a) are not to be rendered redundant, they must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances[50].**

On this basis it could be argued that a hosting company, by deploying IRTs to identify images of child abuse on its servers, has discharged its obligation to act in a diligent manner; and therefore is entitled to rely on the liability shield of Article 14 in respect of any subsequent illegal images found on its service. By using IRT, in other words, a provider could reasonably expect to rely on the exemption in relation to any images bypassing the IRT. The converse of this argument, consistent with the reasoning in *L'Oreal*, is that a provider that might easily have deployed an IRT that would have identified relevant images, *'should have identified the illegality in question'*.

It should not be assumed that the risk of liability founded in constructive knowledge or a lack of

[49] L'Oreal, at para. 120.
[50] Ibid., at para 121.
[51] Section 10(5), Information Society Services Law published in OJ No. 183 of 17 November 2004.
[52] Electronic Commerce Act (CAP. 426) 2002, at s. 21(1).

due diligence is confined to claims for civil damages. Some member states (Czech Republic, Hungary, Latvia, Malta, Poland, Slovakia, Spain) have not distinguished between criminal and civil liability. Under Latvian law, for example, the condition for exemption is that a host provider does not have access to data, which 'may indicate illegal activities or information.'[51] Malta restricts the exemption to liability for damages[52].

While knowledge or awareness must relate also to the legality of the information itself, images of child abuse may be considered to lie at the opposite end of a spectrum of illegal content from allegations of intellectual property infringement, where more complex questions of fact and law may arise. In France for example an appeal court has held that all racist, anti-Semitic or child abuse material met the criterion of 'manifestly illicit[53].' The Belgium Supreme Court has held that the domain owner and operator of a website containing hyperlinks referring to images of child abuse had control and knowledge of these illegal hyperlinks even where the hyperlinks were inserted by others, resulting in the denial of the liability exemption[54].

Courts have held that the circumstances of a case and the nature of the illegality alleged will influence the form of notification required for a company to take action. A Dutch Court, for example, has stated that a 'simple notification' could confer 'actual knowledge' on the part of the intermediary where the content is 'unmistakably' illegal[55]. EU member states have adopted different approaches to notification. Some stipulate a number of formal requirements sometimes amounting to a statutory notice and take-down procedure; others do not, so that any informal correspondence has the potential to compromise the shield. However, even where a formal procedure is prescribed, the courts have sometimes been prepared to adopt a more flexible approach. Whereas Spain's e-commerce law[56] implies that notification needs to come from 'a competent body', in the case of *SGAE (General Society of Authors and Editors) v Asociacion de Internautas ('Internet Users Association')*, the intermediary was held liable for defamatory contents hosted on its website without any such notification from such a body (a ruling eventually upheld by Spain's Supreme Court).

More recently the High Court in Northern Ireland, *CG v Facebook Ireland Limited and Joseph McCloskey*[57], considered the linked issues of notice and knowledge in the context of a claim brought by a man previously convicted of a number of sex offences. A Facebook page had been created by the second defendant designed to identify and incite reprisals against individuals

[53] FR44. – CA Paris, 08/11/2006, Comité de défense de la cause arménienne c/ M. Aydin S., SA France Télécom services de communication résidentiels, http://www.foruminternet.org/telechargement/documents/ca- par20061108.pdf; Recommandation Les enfants du Net II : Pédo-pornographie et pédophilie sur l'Internet, 25 janvier 2005, http://www.forumInternet.org/recommandations/lire.phtml?id=844
[54] BE20. – Cour de cassation, 3.2.2004, R.D.T.I., 2004, n° 19, n° P.03.1427.N, (V.R. c. ministère public).; En première et seconde instance : BE18. – Tribunal de première instance d'Hasselt (correctionnel), 1.3.2002, Inédit, (ministère public c. V.R.) ; BE19. – Cour d'appel d'Anvers, 7.10.2003, n° 440 P 2002, A.M., 2004, liv. 2, pp. 166 et s., (V.R. c. ministère public).
[55] NE11. – District Court of Haarlem, 11/09/2003, Lycos Netherlands BV vs Mr Pessers, LJN number AL1882, case number 94609/KG ZA 03-426, disponible via www.rechtspraak.nl; NE12. – Appeals Court of Amsterdam, 24/06/2004, Lycos Netherlands BV vs Mr Pessers; NE13. – Supreme Court, 25/11/2005, Lycos Netherlands BV
[56] Article 16.1(b)
[57] 2015 NIQB 11

with such convictions. A claim by a previous individual had resulted in a court order for the page to be taken down, whereupon the second defendant established a new page under an only slightly modified banner (i.e. 'Keeping Kids Safe from Predators 2'). Finding for the claimant, the court held that the first defendant should have taken action even without a letter of complaint:

> **I consider that the first defendant had the capacity, resources and knowledge to look for and to assess material in relation to CG on the second defendant's profile/page without receiving any letter of claim or any complaint from CG.**[58]

The underlying principle appears to be this: in certain circumstances, where a company is clearly in a position to identify and take action against manifestly illegal content, it will not be a defense to assert lack of knowledge.

Indeed such a principle can draw support from a number of the Recitals to the ECD, in particular Recital 40 ('service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities'). It might even be argued that the failure to deploy readily available crime prevention techniques amounts to either 'wilful blindness', a form of knowledge, or aiding and abetting, on the basis that omitting to deploy IRTs knowingly facilitates the criminality in question[59]. While such an argument may seem slight, it does present a potential risk for hosting companies declining to use available IRTs. In the event that a provider was found to be hosting images of child abuse, a court could find that the provider *could and should* have known about them, and therefore that they are not in a position to rely on the exemption from liability.

4.1.4 Notice and Take-Down (NTD)

At the time of ECD's adoption it was decided not to establish procedures for 'notice and take-down'. Rather Recital 40 and Article 16 appear to encourage self-regulation in the field. Such flexibility has come at the price of legal certainty. Given the conflicting interests at stake (for example between copyright holders and the telecommunications industry) it seems unlikely that consistent practices across the EU will emerge on a voluntary basis.

The functioning of ECD Article 14 (as distinct from the Article itself) was criticized during a public consultation on the ECD, launched by the European Commission in 2010. The responses are summarized in an EU Staff Working Document from 2013[60]:

[58] at para. 61
[59] Note that Recital 44 refers to liability for those that 'deliberately collaborate' with a user in their illegality; although this is only applicable to the 'mere conduit' and 'caching' activities of intermediaries. An examination of accessory liability is beyond the scope of this report
[60] Commission Staff Working Document, E-commerce Action Plan, 2012-2015, Brussels, 23.4.2013

> **....the vast majority and a wide variety of stakeholders indicated, in their contributions to the consultation, that changing the E-commerce Directive (ECD) would be undesirable. However, they also indicated that the functioning of notice-and-action procedures, in the context of Article 14 ECD, should be improved. In particular they considered that there is too much regulatory fragmentation and legal uncertainty, growing costs due to inefficiencies, too many instances of too slow action against illegal content and instances of action against legal content.**

In response, the Commission announced an initiative regarding 'notice-and-action' procedures[61]. In June 2012, the Commission launched a further consultation specific to Notice and Action procedures for notifying and acting on illegal content hosted by online intermediaries [62]. As yet only a selection of responses have been published. Most of these agree that different categories of illegal content require different approaches: given the variety of illegal content online, a homogenous response system is unlikely to result in proportionate interventions. Respondents also noted that critical terms in the ECD such 'actual knowledge', 'awareness' and 'expeditiously' were ambiguous, and that the scope of the term 'hosting' is insufficiently clear[63].

Taken as a whole, it seems reasonably clear that the ECD was not intended to disincentivise targeted monitoring for the purpose of removing and 'stay-down' in respect of specific forms of illegal content such as images of child abuse. Indeed the use of technology to counter such images may well have been envisaged in a number of its Articles and Recitals. The ECD also encourages the use of voluntary agreements and codes of conduct in this area. A EU-wide framework on 'Notice and Action' would support the ECD objectives of consistency and legal certainty in this area, and is to be recommended.

4.1.5 Court orders and technical measures

Part of the rationale for deploying IRTs is the avoidance of costly and time-consuming court proceedings. This section will therefore clarify the circumstances in which a provider might find itself subject to court proceedings if it elects not to deploy IRTs.

As ECD Article 14(3) makes clear, the exemptions from liability do not preclude injunctions requiring intermediaries to take appropriate action against unlawful content:

[61] DG Market, 'Initiative on a clean and open Internet: procedures for notifying and acting on illegal content hosted by online intermediaries' (June 2012).
[62] See http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm
[63] See ICRI Working Paper 21/2015, Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, Aleksandra Kuczerawy

> **5. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.**

Recital 45 refers specifically to the possibility of injunctions:

> **The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.**

The majority of Member States[64] have directly implemented s. 14(3) ECD.

The Austrian Supreme Court ruled that Austria's legislation only exempted a defendant from possible liability for damages and criminal prosecution, and does not prevent claims for injunctive relief under civil law[65]. Likewise in the UK case of *Bunt v Tilley*, the court held that the relevant provisions of the Electronic Commerce Regulations 2002 did not preclude the granting of an injunction, because they were only designed to restrict the imposition of financial and penal sanctions[66].

In Germany the Federal Court of Justice has ruled that a host provider, which had obtained notice of an infringement, not only had to remove the unlawful content, but had to take all technically feasible and reasonable precautions to prevent future infringements[67]. Furthermore, the monitoring obligation should not be restricted to a specific piece of illicit content or activity but rather covers all the infringements that appear to be essentially similar to the original infringement (referred to as the 'core theory')[68].

The extent of any specific monitoring obligations will usually depend on the circumstances of the case, including the economic and technical feasibility of the proposed measures, such as deploying IRTs. However, the degree to which a court will be willing to give consideration to the economic implications of a technical measure for a web-host may differ where child sexual

[64] Austria, Cyprus, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, the Netherlands, Slovakia, Spain, UK
[65] HG Wien, 21/6/2006, 18 Cg 67/05, http://www.internet4jurists.at/entscheidungen/hg67_05w.pdf
[66] [2006] EWHC 407 (QB), at para. 56.
[67] BGH, 11/3/2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I.
[68] See Verbiest, T., Spindler, G., Riccio, G., and Van der Perre, Study on the Liability of Internet Intermediaries, 2007 ('Liability Study'), at p. 71. The authors would like to acknowledge the assistance of Giovanni Riccio in supplying an update to this 2007 Commissioned-funded study.
[69] Case C-132/12, [2014] 2 All ER (Comm) 301, at para. 99.

abuse images are concerned compared with those of copyright infringement. In the recent *Google Spain* decision, for example, the Court of Justice asserted that protecting fundamental individual rights (i.e. privacy) overrides 'as a rule' the economic interests of providers[69]. While copyright infringement primary engages the economic interests of the rights-holder seeking the order, a different order of interests would seem to be engaged when addressing child sexual abuse images.

In another German case relating to an access provider, the injunction requiring the provider to block access to a pornography website did not specify the necessary technical measures to be taken. The access provider used DNS blocking rather than the blocking of IP addresses to avoid inadvertently blocking sites outside the scope of the order. Although it was recognized that the technique could be circumvented, this was not considered to be a fundamental objection to the order: the technique would still impede access for a significant number of users[70].

When courts in Belgium and Spain have ordered intermediaries to remove illicit content or to disable access, the relevant technical measures have not been specified[71].

Although injunctions relating to images of child abuse do not feature specifically in the case law, it is evident that they might arise in one of two contexts. First, the victim of child abuse, their representative, or a national supervisory authority, aware that images are in circulation, might obtain an injunction on the basis that the image, as personal data, is being unlawfully processed. Second, and more likely in the context of a larger data set, child protection authorities might seek an order under national child protection legislation.

The German courts have developed a doctrine of 'accessory liability' as a basis for injunctions against intermediaries. Consequently legal responsibility for unlawful content is extended to all persons who causally contribute to the infringement of a third party's right, provided they have an effective means of preventing the infringement – subject to the existence of a 'duty to examine'[72] (the existence of which will depend on a variety of circumstances). Non-profit-making services, for example, are widely exempted from the duty[73].

The German administrative courts have endorsed orders issued by state providers against access providers by ordering them to block access to Nazi propaganda websites. The Higher Administrative Court of Munster confirmed these injunctions as a suitable means to obstruct

[70] OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 – Düsseldorfer Sperrverfügungen.
[71] Tribunal de première instance de Bruxelles, 29.06.2007, (SABAM c. Scarlet), N° 04/8975/A, inédit; – Tribunal de première instance de Bruxelles (cessation), 5.9.2006, www.droit.be, n° 2006/9099/A, (CopiePresse c. Google); . – Cour d'appel de Liège (réf.), 28.11.2001, J.T., 2002, liv. 6051, pp. 38 et s; Decision (Sentencia) n° 00126/2005 of the Court of first Instance of Madrid (n° 42), June 15th, 2005 – SGAE (Sociedad General de Autores y Editores v. Asociación de Internautas ; – Decision (Sentencia) of the Provincial Court of Madrid (Section 19), February 6th 2006, Appeal request n° 841/2005 – Affaire Asociación de Internautas v. SGAE (Sociedad General de Autores Editores) ;
[72] Köhler, in: Hefermehl/Köhler/Bornkamm, § 8 UWG Rn. 2.12.
[73] BGH, 17.5.2001, I ZR 251/99, MMR 2001, 671 – ambiente.de.
[74] OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 – Düsseldorfer Sperrverfügungen.
[75] VG Arnsberg, 6.12.2002, 13 L 1848/02 (court of lower precedence to OVG Münster, 19.3.2006, 8 B 2567/02, MMR 2003, 348 - Düsseldorfer Sperrverfügungen); VG Köln, 3.3.2005, 6 K 7151/02, MMR 2005, 399; VG Düsseldorf, 10.5.2005, 27 K 5968/02, MMR 2005, 794; VG Minden, 31.10.2002, 11 L 1110/02, MMR 2003, 135 VG Düsseldorf, 19.12.2002, 15 L 4148/02, MMR 2003, 205.

the proliferation of Nazi propaganda in Germany[74]. The Courts have considered such orders to be reasonable and proportionate since the blocking of the content was technically feasible[75]. It was left to the provider to find the appropriate means to accomplish this task.

In Spain LSSICE Provision 8.1 authorises the competent authorities to take appropriate measures to restrict an information society service for:

a) the protection of public order, criminal investigations, public security and national defence;

b) the protection of public health;

c) the protection of dignity and the principle of non-discrimination;

d) the protection of young people and children.

There is little doubt that the circulation of images of child abuse constitutes 'inhuman or degrading treatment' within the scope of ECHR Article 3, and a serious invasion of the 'right to privacy' under ECHR Article 8. On that basis Strasbourg jurisprudence implies a positive obligation on Member States to implement appropriate preventative measure[76]. In general terms, therefore, the availability of injunctions or civil orders requiring action against images of child abuse is to be expected.

There is, however, a more specific question as to whether an order against an information society service to deploy IRTs would be consistent with ECD Article 15 (*'No general obligation to monitor'*), which provides as follows:

> **1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.**
>
> **2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request,**

[76] X and Y v Netherlands ECHR 8978/80, 1985.
[77] Eg Denmark, Finland, Spain, Ireland, UK and the Netherlands.

> **information enabling the identification of recipients of their service with whom they have storage agreements.**

Whereas some member states have directly implemented Art 15(1), others have not[77]. In consequence of its incorporation of Art 15(1) in 2006 Luxembourg repealed what was previously section 2 of its E-commerce Law, which required host providers to monitor for certain categories of content (including child abuse images).

Article 15(1) is qualified by Recital 47, which states:

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

The question, regarding the impact of Article 15(1) on the deployment of IRTs, might be subdivided as follows:

(a) Do IRTs necessarily entail the monitoring of the entirety of a hosting company's user data?

(b) If so, would an order to deploy an IRT necessarily amount to 'a general obligation to monitor' for the purposes of Art 15(1)?

(c) If so, could such an order be justified where sought 'by national authorities in accordance with national legislation'?

There are a number of authorities bearing on question (b) above. Since they do not relate specifically to IRTs, and generally concern civil claims rather than orders sought 'by national authorities', they do not however assist with questions (a) and (c).

In *Scarlet Extended SA v SABAM*[78], SABAM, a management company representing various artists, sought to prevent Scarlet, a company providing its customers with access to the internet, from facilitating breaches of its clients intellectual property rights. Specifically SABAM argued that Scarlet should install a filtering system across its services. The following question was referred to the Court of Justice:

> **Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental**

[78] C-70/10, [2011] E.C.R. I-11959.

> **Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: 'They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right', to order an [ISP] to install, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?**

In considering the effect of Article 15(1) the Court held as follows:

> **the Court has already ruled[79] that the prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement *of intellectual-property rights*** [emphasis added]**. Further, such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48[80], which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.**

Unsurprisingly the Court reached the same conclusion on similar facts, in another case involving SABAM[81].

It is evident from these judgments that courts, in the context of Art 15(1), are likely to be wary of orders that entail wholesale monitoring. The concerns relate not only to the economic impact on the provider, but also to users' rights to protection of their personal data, and their freedom to receive or impart information[82]. Nevertheless *Scarlet v Sabam* is not authority that an order entailing comprehensive monitoring can never be imposed. The judgment is carefully circumscribed within its intellectual property context; and the balance of interests will be different where an order is required to prevent breaches of ECHR Article 3.

Even in the context of intellectual property infringement the High Court of England and Wales

[79] I.e. in L'Oreal SA v eBay, ECJ, 2011, C-234/09.
[80] concerning the enforcement of intellectual property rights.
[81] SABAM v Netlog NV (C-360/10), [2012] 2 C.M.L.R. 18
[82] See Scarlet v SABAM para. 50.
[83] Twentieth Century Fox Film Corp & ors v British Telecommunications Plc [2011] EWHC 1981.

has ruled that filtering does not contravene ECD Art 15(1) unless it involves 'active monitoring'[83]:

> **The order sought by the Studios does not require BT to engage in active monitoring……, but simply to block (or at least impede) access to the Newzbin2 website by automated means that do not involve detailed inspection of the data of any of BT's subscribers. To the extent that this amounts to monitoring, it is specific rather than general. Furthermore, it would be imposed by a case-specific order made under national legislation which implements Article 8(3) of the Information Society Directive.**

In summary, it would certainly be possible to distinguish an order requiring the implementation of IRTs from the circumstances in *L'Oreal v eBay and Scarlet v SABAM*. Web-hosts may also prefer to avoid litigation carrying any suggestion of complicity in the sexual exploitation of children.

Finally it should be noted that Article 15(1) does not, of course, prevent a web-hosting company from conducting 'general monitoring' on a voluntary basis; although it would need to have obtained the contractual authority and consent of its users to engage in such conduct or may risk exposure under data protection law (see below) or under other heads, as well as losing the benefits of Article 14(1). Obtaining user authority and consent through terms of service, 'acceptable use' and privacy policies is standard practice in the industry[84]. Whether such practices are valid and effective is, however, beyond the scope of this report.

4.1.6 Duties of care and proactive measures

As indicated by Recital 48 of the ECD, where a member state has imposed a duty of care on providers to take action against specific forms of illegal content, this will override the Article 14 exemption from liability:

> **This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.**

[84] Even among those found guilty of facilitating large-scale copyright infringement! See BREIN v. Mininova, Rb. Utrecht 26 August 2009, LJN BJ6008, 250077 / HA ZA 08-1124, in which the court found that Mininova did police the content made available via its site, in line with its terms of use.

In relation to the protection of children there are various instruments that may underpin the imposition of such duties of care under national law, including Article 24(2) of the Charter of the Fundamental Rights of the European Union:

> **In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.**

Further, on the assumption that the processing of images of child abuse constitutes 'inhuman or degrading treatment', ECHR Article 3 ('Prohibition on torture') requires states to introduce measures to prevent such processing, even by private parties[85].

Article 25 of the Child Protection Directive ('Measures against websites containing or disseminating child pornography') provides that:

> **1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.**

> **2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.**

Paragraph 1 would seem to provide a legal basis for Member States to impose a specific duty on web-hosts within their jurisdiction to deploy 'reasonable' technical measures to identify and remove child sexual abuse material. While paragraph 2 recognizes the need for transparency, something referred to previously with respect to a web-host's ToS and AUP, adequate safeguards need to be implemented at each stage of IRT deployment, from database assembly to reporting procedures.

In Sweden the Law for Electronic Bulletin Boards[86] imposes on bulletin board operators what appears to be a general obligation to control and monitor the content of their websites (including

[85] Z & others v UK 34 EHRR 3, 2001, at para. 73
[86] Act on Responsibility for Electronic Bulletin Boards, 1998:112; http://www.sweden.gov.se/content/1/c6/02/61/42/43e3b9eb.pdf
[87] Liability Study, at p. 70.

images of child abuse). The Government referred to Recital 48 of the ECD in passing it. In practice, however, it is understood that the obligations might be met by proportionate measures such as carrying out periodic checks or installing (and acting on) a complaints page[87].

In Italy, specific legislation on child abuse images[88] requires access and host providers to report relevant information to the National Centre for the Prevention of Internet Child Pornography; and provides for the Ministry of Communication and the Ministry of Reforms and Innovations in Public Administration to introduce supporting technical measures (resulting in a 2007 Decree[89]).

A court in Holland[90], referring to German case-law, stated that injunctions are not affected by the liability exemptions of the ECD. Consequently hosting providers have a 'duty of care' to prevent and terminate infringements. In this case a notice and take-down procedure was held to be sufficient to meet the standards of care, taking into account the costs of proactively monitoring its web-sites.

In the absence of alternative proactive measures, a decision not to deploy available IRTs might be seen to conflict with the existence of any duty of care

4.2 Liability under data protection law

The ECD states that it does not provide exemption from liability for breaches of data protection legislation[91]. Consequently web-hosting companies need to give separate consideration to the risk that inadvertent hosting of child abuse images could put them in breach of data protection provisions. Clearly the processing of images of child abuse would seem a *prima facie* breach of data protection legislation.

The application of data protection legislation to a search engine provider was recently considered by the Grand Chamber of the ECJ in *Google Spain SL and another v Agencia Espanola de Proteccion de Datos (AEPD) and another*[92] (the 'right to be forgotten' case). The first issue for the court to consider was whether Google was engaged in the 'processing' personal data. Under the General Directive, 'processing' is defined in the following terms:

[88] Article 14 of the Law No. 269 of 1998.
[89] Art. 3, this decree was passed on January 2, 2007, and it is entitled "Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto della pedopornografia", http://www.comunicazioni.it/it/index.php?IdPag=1177. District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, disponible via www.rechtspraak.nl; see also NE 16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, accessible via www.rechtspraak.nl
[90] District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, disponible via www.rechtspraak.nl; see also NE 16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, accessible via www.rechtspraak.nl
[91] Recital 14 and Article 1(5)(b). We note that the Commission's proposed Regulation on data protection (January 2012) does attempt to reconcile the two regimes, at Art. 2(3).
[92] Case C-132/12, [2014] 2 All ER (Comm) 301.

> **any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[93];**

Such a broad definition would clearly include the storage of data by a web-hosting provider, as it was held to apply to activities of search engines.

The second, more important, issue to determine is the status of the web-hosting provider under the General Directive, as either a data controller or data processor. Under the current regime, the regulatory obligations primarily reside on the data controller, with the data processor being made subject to contractual constraints[94]. As such, the General Directive can be viewed as establishing an analogue of the regime under Section 4 of the ECD, since data processors are immune for liability as long as they comply with their contractual obligations and do nothing that could render them a data controller in their own right. This binary distinction is likely to dissolve under the new proposed Regulation, with data processors becoming subject to direct regulatory obligations and 'jointly and severally liable' for damage arising from a breach of the data protection rules[95].

A data controller is the person "which alone or jointly with others determines the purposes and means of the processing of personal data"[96]. In *Google* Spain, the Court considered whether the search engine should be regarded as a 'data controller' and answered in the affirmative, on the following basis:

> **the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page[97].**

In explaining its reasoning the court emphasizes the Directive's objective of 'complete protection for data subjects', stating at para. 34:

[93] Directive 95/46/EC 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (OJ L 281/31, 23.11.1995)('General Directive'), at art. 2(b).
[94] Ibid., at art. 17(3).
[95] Commission draft of the proposed Regulation (January 2012), at art. 77(2).
[96] General Directive, at art. 2(d).
[97] Google Spain, at para. 35.

> **it would be contrary not only to the clear wording of that provision but also to its objective – which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects – to exclude the operator of a search engine from the definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.**

By contrast, the Advocate General, in his non-binding opinion to which the Court did not refer, concluded that a search engine operator should *not* be regarded as a data controller, since it "cannot in law or in fact fulfill the obligations of controller"[98].

For our purposes, the issue for consideration is the extent to which web-hosting services can be distinguished from those of a search engine. On the one hand, it may be impossible to generalize, since the nature of the relationship between a web-hosting provider and its users will always depend both on the precise nature of the service and activities carried out by the provider, as well as the ToS governing the relationship; although, as has been made clear previously, it is the former that is determinative, not the latter[99]. On the other hand, web-hosting in its most basic form, would seem to clearly fall within the concept of a 'data processor':

> **a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller**

The user makes the decision to place data with the web-host, who stores that data and makes it accessible to the user on demand, and the user determines what types of data are stored and what purpose(s) is made of that data. As the Article 29 Working Party has noted, of the two components that a controller 'determines', the purpose is always reserved to the controller, while the exact means "can be delegated by the controller, as far as technical or organizational questions are concerned"[100]. Indeed, the concept of 'data processor' would seem to chime somewhat with the Court of Justice's opinion that 'hosting' should be a neutral role "in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores[101]."

The Article 29 opinion also notes, however, that the person that decides "who has access to the data processed" shall be considered the controller. In the context of an IRT deployment, therefore, the web-host would need to ensure that the user, as 'controller', has contractually agreed to its deployment and any disclosure consequent to any detection, whether it be to an

[98] Opinion of Advocate General Jääskinen, delivered on 25 June 2013, at paras 76-100.
[99] See Article 29 Working Party Opinion 10/2006 'on the processing of personal data by SWIFT' (WP128), at 3.1.
[100] See Article 29 Working Party Opinion 1/2010 'on the concepts of "controller" and "processor"' (WP169), at para. III.1.b.
[101] Google France & ors v Viaticum & ors [2010] E.T.M.R. 30, at para. 114.

independent body or a law enforcement agency. In the absence of such an agreement, made in accordance with Article 17(3), the web-host risks being considered a controller in its own right and would be subject to all the obligations applicable to a controller.

The risk of liability under data protection legislation was apparent in the 2015 case of *CG v Facebook Ireland Limited*. Here it was accepted that Facebook Ireland would be a 'data controller' for the purposes of the Data Protection Act. The court held that it had no justification for processing sensitive personal data regarding the claimant; that the claimant had suffered distress as a result; and that Facebook Ireland would have no defence to a claim for damages. On the facts, however, the court declined to find a breach of the Data Protection Act on the basis that Facebook was not subject to it as a result of being incorporated in the Republic of Ireland. It was only in relation to the distinct claim of misuse of private information that the court considered the effect of ECD Article 14, holding that on the facts of the case it did not exempt Facebook Ireland from liability in damages[102].

5. IRT deployments and legal risk

Assuming the existence of practical, effective technology, there are risks in a decision to use it or not to. Both sets of risks need to be considered to provide a balanced overview to support informed decision-making by host providers. While the previous the section highlighted the limits and uncertainties surrounding reliance on Articles 14 and 15 as a basis for inaction, in this section we assess the risks of deployment.

5.1 Risks from identifying illegal content

The confidentiality of communications is inherent in the right to privacy under Article 7 of the Charter on Fundamental Rights. It is also the subject of more specific legislation including EU Directive 2002/58/EC (Directive on privacy and electronic communications), Article 5(1) of which states:

> **Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by**

[102] See also the Italian Supreme Court decision in the Google-Vividown case: Court of Cassation, sess. III Penal, sentence no. 5107/14; filed on 3 February 2014; available at http://www.giurcost.org/casi_scelti/Google.pdf (in Italian)

> **persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1).**

As noted previously, however, this provision is limited in its application and may not be applicable to the provision of web-host services. However, European Union law contains provisions criminalizing those that compromise the confidentiality, integrity and availability of information systems. In a Directive 'on attacks against information systems', Member States are required to criminalize illegal access to computer systems:

> **Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor[103].**

It also requires the criminalization of illegal interception:

> **Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor[104].**

Working on the presumption that IRTs primarily operate on the content of the hosted material rather than the related metadata, their use may, in certain circumstances, constitute interception. Whether or not it does will depend on a combination of the detail of national law, the technology and the way that it is deployed. National law in this area tends to complexity, and does not always apply neatly to digital technologies.

Both offences require any access or interception to be 'without right' defined in the following terms:

> **not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.**

In terms of illegal access, the web-host should be able to obtain such an entitlement to access

[103] Directive 2013/40/EU (OJ L 218/8, 14.8.2013), at art. 3.
[104] Ibid., at art. 6.

the hosted content for the purposes of deploying an IRT, through its ToS. Where such access constitutes interception, then consent would usually be required from both parties to the communication, which would be problematic for the web-host, who will often not have a relationship with both parties. To address this legal risk, some form of public law provision may need to be relied upon, either in the form of a statutory entitlement to access for specified purposes, or a statutory defence to liability. The issue should also be covered in any governing arrangement with the competent authorities (see 6.2 below).

Assuming the hosted material includes communications, one consideration may be whether the communications, at the point of the intervention, are, in the language of the UK's *Regulation of Investigatory Powers Act* (RIPA) 'in the course of their transmission'. Although the traditional concept of 'interception' applies to communications in progress (eg a live phone call, or a letter en route from A to B), national law may broaden the definition. RIPA s.2(7), provides an example:

> **For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.**

Interception will not necessarily require independent authorization to be lawful. RIPA s. 3(3), for example, provides for providers of telecommunication services to conduct interception without warrant in the following circumstances:

> **(3) Conduct consisting in the interception of a communication is authorised by this section if—**
>
> **(a) it is conduct by or on behalf of a person who provides a postal service or a telecommunications service; and**
>
> **(b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.**

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

More generally, the risks of breaching such provisions designed to protect privacy must be kept in perspective. The rights to privacy and confidentiality of communications are clearly not absolute. Hosting or processing images of child abuse is itself a serious infringement of the right to privacy of the victims. Given the 'manifest illegality' of images of child abuse, and the limited intrusion into privacy represented by an automated check against known images, the use of IRTs is likely to be considered necessary and proportionate in pursuit of the legitimate objectives. National law might be expected to provide accordingly.

A company's ToS should be explicit that measures will be taken to identify, remove and report any images of child abuse. Use of IRTs should not generally be undertaken as a 'tasking' from law enforcement; rather it should be regarded as the mechanism for enforcing a company's terms and conditions of service; and preventing its complicity in the illegal sexual exploitation of children. As long as the use of IRTs is flagged in this way, for the limited purpose of identifying known images of child abuse, customers are unlikely to consider them a significant threat to privacy.

5.2 Risks from handling illegal content

The nature of any enquiry into 'hosting' liability can be considered as a series of questions. First, does the conduct of the person with respect to the illegal content attract potential liability, whether primary or secondary[105] in nature? If so, does the substantive law governing that form of conduct contain limitations of liability, in whatever form (e.g. as a defence), which would protect intermediaries engaged in 'hosting'? If not, then is the web-host nevertheless able to rely on the more general protection of Article 14?

As noted previously, under European Union law, Member States are required to make it an offence to possess or distribute images of child sexual abuse. While national laws are not designed to catch those taking action against images of child abuse, they may inadvertently do so. Indeed, this was the situation in the UK, for example, until reforms were introduced in 2003. Prior to the reforms, a web-host that identified an illegal image could be held to have 'made' that image simply in the course of it being viewed for the purpose of reporting it to the police. Although the likelihood of prosecution was slight, it remained a risk. To mitigate that risk, a statutory defence was adopted, where the image was made "for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world"[106].

The general defence of Article 14(1)(b), that "the provider, upon obtaining such knowledge or

[105] I.e. accessory liability.
[106] Protection of Children Act 1978, s. 1B.
[107] Section 6(4) Electronic Commerce Act No. 22/2004 JO of 3 December 2003

awareness, acts expeditiously to remove or to disable access to the information", has been implemented by different states in different ways. Slovakia's Electronic Commerce Act provides an exemption only where the illicit information is removed (but not where access is disabled)[107]. In Sweden, this exemption depends on host providers preventing 'further dissemination' of illegal content[108]. In Finland, the shield only applies where the provider disables access to the illicit content[109].

In any event, Article 14(1)(b) has not been tailored to take into account the possible needs of a subsequent criminal investigation. The detection of an image of child sexual abuse may be vital evidence of abuse in the physical world. It will not be enough simply to remove or block access to identified images. For obvious reasons, the web-host may need to retain, collate and forward relevant forensic material linked to the detected content to the competent authorities.

Rather than getting too deep into the technicalities, however, and the variations from state to state, the essential considerations can be expressed in general terms.

It is to be hoped that the IRTs function so as to confine a web-host's responsibility to installation of the software (e.g. by forwarding all positive hits directly to the competent authorities for assessment). Clearly it is preferable that web-host's staff has neither access to the images themselves nor any role in their assessment.

In the event that the operation of the IRTs permits or requires company staff to have access to the images, it is essential that such access be subjected to rigorous controls and safeguards. *Inter alia*, given the distressing nature of such images, no member of staff should be required to view them, and any volunteer should be subjected to psychological assessment and vetting.

The overarching point, however, is that clear, written arrangements governing the use of IRTs should be agreed with the competent authorities.

5.3 Risks from inappropriate disclosure of filter-generated data

Disclosure of innocent customer data, whether accidental or deliberate, may constitute a breach of confidentiality (contractual or otherwise), privacy or data protection obligations. Disclosure for law enforcement purposes will generally be permissible[110], although such exemptions may not be applicable to false positives, especially if the web-host was held not to have exercised sufficient care with respect to the disclosure.

The risk of inappropriate disclosure by a web-host provider will depend both on the accuracy

[108] Electronic Commerce Act section 18
[109] Finnish Act 457/2002 of 5 June 2002 on the Provisions of Information Society Services available at www.finlex.fi/fi/laki kaannokset/2002/20020458)
[110] E.g. General Directive, at art. 13(1)(d).

and effectiveness of the IRT in question, as well as the procedures that it implements to handle the data generated through its operation. As noted in Section 2, the accuracy will depend on the specific workings of the IRT in question. While the web-host may seek contractual guarantees and indemnities from the IRT provider, these are likely to be strongly resisted by the provider. However, on the assumption that any 'hits' are forwarded to the relevant authorities for actioning, it should be for those authorities to identify any 'false positives' and handle the data appropriately.

With regard to its procedures, the web-host, whether as data controller or processor, will have obligations (regulatory or contractual) to implement 'appropriate technical and organizational security measures'[111]. These measures must reflect the risks and the nature of the data, which in this case would seem to impose a high standard.

5.4 Risks from not disclosing filter-generated data

The risks under this heading can arise when the web-host becomes aware of illegal images, through its deployment of IRTs against the content it hosts, but then fails to report such findings to the appropriate authorities.

Intermediary reporting requirements can be subdivided into rules that impose a proactive monitoring obligation upon the intermediary and those that are reactive in nature, arising only when the intermediary has become, or been made, aware of the illegality. Some jurisdictions require that Internet service providers report child abuse images to the authorities as soon as they 'obtain knowledge'[112] or become 'aware'[113] of their existence, backed by criminal sanction for a failure to report. Among EU Member States, Italy imposes specific reporting obligations in relation to child sexual abuse images[114]; while under Czeck and Slovak law, providers are expected to proactively reveal identified breaches of criminal law more generally[115].

Where an image is identified, it may give rise to a duty of care regarding the children at risk from the associated individuals. As such, the risks under this heading can be seen as being closely aligned with the duty of care referred to at Recital 48 of the ECD and discussed earlier (at 4.1.6).

In less legalistic terms, a web-host will want to ensure appropriate action is taken whenever an image is identified. The essential point here is a straightforward one: positive hits need to be notified to the competent authorities, and supporting arrangements should be agreed in advance of IRT deployment. One potential concern for the authorities may be the volumes

[111] Ibid., at art. 17(1).
[112] United States Federal law at 42 USC § 13032 ('Reporting of child pornography by electronic communications service providers').
[113] Australian Criminal Code Act 1995, at s 474.25 ('Obligations of Internet service providers and Internet content hosts').
[114] Law of 3 August 1998, No. 269, at art. 14.
[115] Liability Study, at p. 40.

that any reporting requirement produces, especially where the deployed IRT is configured in a manner that generates significant numbers of false positives.

6. Mitigation

The previous sections considered the various legal risks arising from the deployment or non-deployment of IRTs. In response to such risks, a web-hosting provider will be concerned to take steps to mitigate any such risks. The following section briefly outlines possible mitigation strategies.

6.1 The risks of a decision not to deploy

As outlined above, article 14 of the ECD does not provide hosting companies with a reliable shield against liability for any images of child abuse they may inadvertently be processing. There is the uncertainty around the definitions of 'hosting' and 'information society service', terms on which the application of the provision depends. Even when Article 14 applies, it may be overridden by specific duties of care and undermined by circumstances in which the provider should have been aware of the illegal content. Nor does it prevent injunctions or civil orders demanding action against illegal content.

Consequently a blanket policy of non-deployment may not be advisable. There are two approaches to risk mitigation. Recognizing the differences in national legal frameworks, a company may choose to deploy IRTs only following a detailed analysis of the legal requirements in a particular jurisdiction. Alternatively, a more robust approach would be the adoption of a policy of deploying IRTs subject to agreeing an appropriate protocol with the relevant national authorities. In so far as the authorities fail to provide the requisite assurances or support an effective working protocol, this, at least in part, would transfer responsibility for non-deployment away from the company.

6.2 Mitigating risks of deploying IRTs

The deployment of IRTs raises sensitive issues regarding both customer privacy and the processing of positive hits.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

All should be manageable by ensuring compliance with national legal frameworks; the incorporation of appropriate provisions in terms and conditions of service; and the establishment of arrangements with the competent authorities for identifying false positives and ensuring appropriate engagement with law enforcement.

7. Conclusions and recommendations

From the foregoing analysis, it should be apparent that the legal risks relating to the deployment of IRTs are different in kind from the risks of non-deployment. On the one hand, the risks of deployment should be capable of mitigation through the establishment of clear processes agreed with the competent authorities. On the other, a deliberate decision not to deploy IRTs, consequently allowing known images of child abuse to remain on the company's system, entails legal and reputational risk that require assessment on an ongoing basis.

We conclude that the use of IRTs will not generally compromise the legal position of a hosting company as long as:

- The arrangement is supported by a clear regulatory (including self- or co-regulatory regimes), an operating framework or memorandum of understanding (MoU)[116] with the relevant competent authorities, governing the appropriate action to be taken in relation to positive hits, protecting the operator, for example, from claims they missed opportunities to prevent serious harm to a child; and
- The company operates within the terms of such (co-)regulation, operating framework or MoU.

Moreover, we note that web-hosts should not presume that they can rely on the ECD Article 14 exemption from liability in relation to any images of child abuse they may inadvertently be processing. As noted, there are a number of reasons for this:

(a) Variation and uncertainty regarding the definition of 'host provider', with consequent uncertainty for the scope of the protection;

(b) Uncertainty as to whether a web hosting company falls within the definition of 'information society service' (and thus within the scope of the protection);

(c) Potential exposure to liability on the basis that the provision of hosting services could give rise to secondary liability;

[116] E.g. in the UK, the 'Memorandum of understanding between the Crown Prosecution Service and the Association of Chief Police Officers concerning Section 46 Sexual Offences Act 2003', available at https://www.cps.gov.uk/publications/agencies/mouaccp.html

(d) The potential for the authorities to apply for injunctions or civil orders against companies (incurring legal and reputational costs); and

(e) The existence, in some member states, of statutory obligations or duties of care requiring proactive measures to be taken to safeguard the welfare of children.

More generally it is counter-intuitive that companies should be prejudiced as a consequence of taking proportionate action against images of child abuse; and this is likely to be a significant policy consideration when courts resolve any ambiguity within national legal frameworks.

There are, however, legal and reputational risks in companies deploying IRTs in the absence supporting procedures or frameworks agreed with the relevant authorities. These include:

(a) Risks from identifying illegal content
(eg unlawful interception and unauthorized access);

(b) Risks from handling illegal content
(eg possession, evidential destruction, unauthorized access);

(c) Risks from inappropriate disclosure of filter-generated data
(eg data protection and breach of confidence);

(d) Risks from not disclosing filter-generated data
(eg reporting obligations).

Internet intermediary companies should not be expected to manage such risks themselves. Rather procedures should be agreed and implemented to make their role as straightforward as possible, handing responsibility for potentially complex decision making (eg screening for 'false positives') to an appropriate intermediary.

It may be that procedures need to be agreed with the competent authorities of individual member states. In the absence of any EU wide standardization or guidance regarding suitable procedures the result is likely to be confusion, inefficiency and an additional resource burden on providers.

We therefore recommend that consideration be given to:

1. The development of an EU wide framework governing the actions to be taken when service providers identify images of child abuse, possibly within the ambit of the European Commission's ongoing 'Notice-and-Action' initiative;

2. The EU legal framework should make clear that the deployment of technological solutions, such as IRTs, to identify and facilitate take-down and stay-down of child

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

sexual abuse images should not itself create liability on the intermediary where none exists under applicable law;

3. The establishment of an independent EU wide body, sitting between industry and law enforcement, to serve as the central collection point for the database of unique IDs that are utilized by IRTs;

4. The establishment of national bodies capable of receiving and handling reports generated from industry's use of IRTs to identify illegal images of child abuse;

5. The European Commission embarking upon a more holistic consideration of the liabilities of Internet intermediaries, including consideration of a specific duty of care in relation to child sexual abuse images and appropriate statutory defences against liabilities. A robust intermediary liability regime is needed to encourage service providers to implement appropriate voluntary measures in the fight against child sexual abuse.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

This project has been funded with the support of the European Commission. This publication reflects the views only of the author. The European Commission cannot be held responsible for any use which may be made of the information contained therein.