Chapter 4 - Sectoral frameworks and the E-Commerce Directive – the enforcement gaps

A. Introduction

Chapter 3 provided an overview of the horizontal framework of intermediary liability at EU level. On the one hand, the legal challenges of the ECD that hinder an effective enforcement against unlawful content arose out of technological and socio-economic changes related to the internet. On the other hand, these challenges are further complicated by the diversity of unlawful content online. The sectoral provisions that govern different areas of content are to a large extent under the competency of Member States, the EU having only indirect or peripheral influence. Exceptions may be the AVMSD, the Infosoc Directive, the new (Copyright) Digital Single Market Directive (DSMD) or the EU consumer protection and product regulation *aquis*.[809] However, some of these provisions only relate to certain aspects of the content in question. Furthermore, the EU exercises peripheral influence in content regulation where EU constitutional principles are at stake. These are mainly the free movement principles[810] and fundamental rights, such as freedom of expression and others protected by the ECHR and the CFREU.[811] The EU also uses soft law instruments for protecting these principles in certain areas of online content regulation, such as codes of conduct or memoranda of understanding. These shall be explored in more detail in the respective content Sections.

Content regulated by Member States' laws may fall under civil and/or criminal law provisions. This may differ between Member States, as much as normative consideration on unlawful content, their enforcement and sanction mechanisms differ. Consequently, there are variations in the application of sectoral content regulation between Member States and this has an influence on the interaction with EU law, and specifically the intermediary liability provisions contained in the ECD. To make matters more

809 Savin (n 384) 115.

810 Treaty on the Functioning of the European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2016) Articles 49, 54, 114.

811 These are usually: ECHR Articles 8, 10; CFREU Articles 7, 8, 11, 16, 17.

complex, the ECD provisions may coexist with specific rules for intermediaries set out in sectoral provisions and with the general rules applied to secondary or intermediary liability through the ordinary law in Member States. The interplay between these various intermediary liability frameworks is complex. As will be shown, national courts tend to prioritise constitutional and national ordinary law principles over EU law.[812] This may partly explain the limited success of the ECD in harmonising online intermediary liability exemption conditions.

This chapter will also demonstrate how the arrival of the internet and online intermediaries has influenced the substantive matter of sectoral law. For example, in copyright the very reliance of the internet on constant copying as a means of "transporting" information and the revolutionary nature of dematerialised, digital copying have gone to the very substance of that law itself. The more detailed analysis of case law in the area of digital copyright and internet intermediaries aims to demonstrate the technical and legal complexities of new intermediation practices on the internet. UGC, content sharing or hyperlinking have all challenged courts, both in the application of copyright law and intermediary liability provisions. Have online intermediaries through which content is shared, become more than just intermediaries in this process? Substantive trademark law, on the other hand, has been less powerfully affected by the trend of digitisation, especially where it concerns the activities of online intermediaries. Only since recent have the vertically integrated activities of online marketplaces started to be seen as affecting the scope of trademark protection directly. However, the superior economic interests at stake in this area have triggered an equally powerful policy debate over the role and responsibilities of online marketplaces. The discussion in this area will dedicate more detail to the various policy initiatives, which started as early as 2011 with the Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet.[813]

In the cases of defamation, hate speech and terrorist material online, the role of intermediaries in amplifying or spreading content or in nudging users to communicate in certain ways may still not make them liable authors with primary responsibility. But could the new quality of facilitation and manipulation of information exchange confer new, extended responsibilities and liabilities on these intermediaries, and if yes, which? In general,

812 Benabou (n 334) 880; Kohl (n 280) 192.

813 'Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet, 2011' (n 665).

the liability of (online) intermediaries in the different content sectors is dependent on the type of content and the specific legal traditions pertaining to secondary or intermediary liability.

Finally, in the area of product and food safety the rise of e-commerce conducted through intermediaries has led to significant enforcement challenges. Online marketplaces and other intermediaries are not the originators of unsafe, non-compliant or illegal products. But do the increasingly vertically integrated activities of e-commerce intermediaries, which may offer advertising, marketing, payments, logistics or financial services to sellers and consumers, affect their responsibilities for the legality of products sold? As lawmakers extend labelling, information and registration requirements onto products sold online and their sellers, does this also affect the obligations of e-commerce marketplaces, which are offering their platforms to thousands or even millions of sellers from across the world?

If this is not difficult enough, then each content sector also engages different fundamental rights. Different unlawful activities and content types may cause different kinds of harms and trigger the public interest in a variety of ways. This may lead to different balancing exercises and outcomes, at both Member State level and by content type, when determining the scope of the responsibilities accorded to online intermediaries. The patchwork of enforcement methods and standards applied against unlawful content can be seen as yet another challenge to the establishment of an effective and predictable common intermediary responsibility framework.

A number of central questions arise out of this heterogeneous picture: Are the ECD's general, horizontal provisions flexible enough to address each sector's and Member State's specific interpretations on the legal protections and responsibilities of online intermediaries? Are there overarching online intermediary principles and characteristics that would justify a horizontal approach to intermediary liability? If yes, how deep should new, horizontally applied principles and responsibilities reach into sectoral frameworks. Should sectoral frameworks be primarily structured by legal area, the harm caused, or by the type of intermediary, or a combination of all?

It is the aim of this chapter to contrast the different sectoral enforcement frameworks of unlawful content and draw conclusions. Given the broad scope of this work, these sectoral overviews can be but introductory and selective. Each sectoral area will be analysed by giving an outline of the legal provisions and competencies at Member State and at EU level. Where relevant, examples will be used to highlight the differences in the substantive laws of the Member States and the impact on enforcement on the in-

ternet. The discussion aims to evaluate the suitability of the current ECD's liability exemption rules and their national transposition in effectively protecting rights at sectoral level and fighting unlawful activity in the specific area. This analysis will include case law, technological trends and developments in private enforcement by platforms, such as the use of filtering or content recognition. Finally, policy trends and developments will be critically reviewed.

This chapter will be a demonstration of how the complex multi-level regulatory set up of the EU has amplified the enforcement problems of the broad, profound and fast transformations caused by the internet. It aims to complement the description of the horizontal legal challenges of the intermediary liability framework described in the previous chapter. These two chapters will serve as a backdrop for the development of a new intermediary responsibility framework, which will be attempted in Chapter 6.

B. Personality rights and public order: defamation, hate speech and terrorist content

1. Defamation

I. Defamation online - background

Together with copyright infringements, defamatory comments belong to the earliest unlawful activities that involved the liability of intermediaries on the internet. Unrestricted online speech was a major achievement of cyberspace for the early Libertarian utopians of the internet. It also influenced early perceptions of cyberspace as a borderless and open medium.[814] As the internet commercialised and became more popular in daily use, however, this free speech ethos created more and more conflicts. Online defamation or libels became more frequent. Comments posted by users against or about others on news servers or bulletin boards[815] or carried through internet access providers[816] caused the first significant legal chal-

814 Edwards, 'The Fall and Rise Of Intermediary Liability Online' (n 119) 51. see also Chapter 2 A

815 Such as the previously discussed *Cubby* (n 371); *Godfrey v Demon Internet Limited* [1999] High Court Of Justice Queen's Bench Division 1998-G-No 30, EWHC QB 240.

816 *Bunt v Tilley & Ors* (2006) [2006] EWHC 407 (QB) (England and Wales High Court Queen's Bench Division).

lenges in courts against the new intermediaries of the internet. Apart from pursuing the actual authors, the complaining parties also went after online intermediaries. They claimed that they were either liable for the defamatory comments as publishers, or that they were negligent as transmitters in failing to remove or prevent unlawful statements.

There are ongoing legal discussions on the role online intermediaries play in defamation via the internet. *Oster*, for example, discusses in relation to common law jurisprudence the view that, if publication is interpreted as an act of communication, then any internet intermediary that participates in this act, simply by virtue of providing the technical facilities, could be seen as a publisher. He notes the basic flaws of the concept of passive intermediary in this context.[817] That view could then be extended to any unlawful acts facilitated in that way by an internet intermediary, putting the intermediary firmly in the chain of responsibility.[818] Under common law rules, online intermediaries, be they IAPs or hosting providers, could seek defences as innocent disseminators of (defamatory) information. Introducing this knowledge element moves the tort of defamation closer to liability for negligence and the exercise of reasonable care.[819] Others, however, define publication more narrowly as acts that confer editorial responsibility and tie the liability of intermediaries for defamatory content to whether they are publishers, subject to strict liability.[820]

In the US, early online defamation cases have contributed to the formulation of the current framework that regulates intermediaries' liability exemptions under the CDA. This Act's almost unfettered immunities of online intermediaries against defamatory content reflect the robust and far reaching free speech protections under the US Constitution's First Amendment.[821] This means that the rights to privacy or protection of personal data succumb more often than not to the right of free speech, which in turn means that intermediaries are less required to intervene in the availability of content.

This balance is somewhat different in the EU. *Pollicino et al* have pointed towards almost diametrically opposite assessments in Europe and the US

817 Jan Oster, 'Communication, Defamation and Liability of Intermediaries' (2015) 35 Legal Studies 348, 354–356, 358. In that context, the "passivity test" under Articles 12 (1) – 14 (1) should rather become a "mere dissemination" test. (358)
818 Benabou (n 334) 871.
819 Oster (n 816) 357.
820 Lipton (n 23) 120.
821 Oster (n 816) 351. Omer (n 493) 301–304.

when dealing with the impact of the internet on fundamental rights:[822] In *Reno v ACLU* the US Supreme Court stressed the importance of encouraging freedom of speech enabled by the internet and assumed that government would be more likely to censor than to promote that freedom. It called therefore for a broad protection of internet intermediaries from liability for third party speech.[823] In Europe, however, the ECtHR stressed, notably in *Shtekel v Ukraine* and in *KU v Finland*, the new risks and harms that content and communications on the internet posed to the fundamental right of privacy. This, it said, outweighed the risk to freedom of expression. Policies regulating the internet had to be adjusted to this new technology in order to adequately protect all fundamental rights.[824]

Although the above cases were judged by the ECtHR, which has no jurisdiction over EU law, many of the ECHR rights and freedoms have been taken over into the CFREU. This includes the two freedoms which are most commonly engaged when dealing with (online) defamation cases: the freedom of expression and the right to a private life. Both have found their way into the online intermediary jurisprudence of the CJEU at several occasions. Given the specific European and EU values, the CJEU, the ECtHR and national courts have traditionally accorded a more measured emphasis to the freedom of speech right than in the US. Consequently, that right has traditionally been restricted more widely by the right to privacy[825] and other rights, such as the protection of personal data[826].

II. The legal framework of defamation in the EU

Apart from the fundamental rights principles, the EU influence on defamation law comes mainly from three areas:[827] the determination of ju-

822 Oreste Pollicino and Marco Bassini, 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis (Ch. 21)' in Andrej Savin and Jan Trzaskowski, *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) 351–352.

823 *Reno v. American Civil Liberties Union* (n 396) para 855. In: Pollicino and Bassini (n 821) 531.

824 *Editorial Board of Pravoye Delo and Shtekel v Ukraine* [2011] ECtHR (Fifth Section) 33014/05 [63] and *KU v Finland* [2008] ECtHR (Fourth Section) 2872/02 [49]. In: Pollicino and Bassini (n 821) 531.

825 A prominent example being *Delfi* (n 777).

826 *Google Spain v AEPD and Mario Costeja González, number C-131/12* [2014] EU:C:2014:317 (CJEU) [97].

827 Savin (n 384) 130.

risdiction in cases that involve international defamation on the internet,[828] the choice of law[829] and, where applicable, the intermediary liability provisions of the ECD. Matters of jurisdiction are probably the most hotly discussed legal issue in online defamation today. There is by now ample jurisprudence by the CJEU that has attempted to interpret the Brussels I regulation in the online context.[830] This subject shall not be treated here. However, the ongoing discussions and disputes on this particular issue just illustrate how much defamation is a transnational phenomenon and how much the internet has influenced this problem.

By contrast, the substantive legal provisions on defamation are not harmonised across the EU and remain under Member States' national competencies. Given different legal and cultural traditions, these substantive provisions may vary considerably. In most Member States defamation may still incur criminal charges, including prison sentences that vary between one and 96 months. However, there is a marked overall trend to decriminalise this offence. In practice, civil sanctions for defamatory acts have become the norm.[831] Defamation law can serve as a useful example for a study on how harmonised framework rules for intermediary liability exemptions interact with national sector laws that may vary significantly not only with regards to normative aspects, but also procedural set-ups and sanction regimes.

828 Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters 2012 Article 7.

829 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations 2007 (OJ L 199). Although this applies only to tort law conflicts.

830 For an overview: Emeric Prévost, 'Study on Forms of Liability and Jurisdictional Issues in the Application of Civil and Administrative Defamation Laws in Council of Europe Member States' (2019) Council of Europe study DGI(2019)04.

831 'Out of Balance - Defamation Law in the European Union: A Comparative Overview for Journalists, Civil Society and Policymakers' (n 479) 7–11. Savin (n 384) 126.

III. Defamation, online intermediaries and the ECD in national law

a. UK

The UK's 2013 Defamation Act[832] deals directly with online intermediaries. In other Member States, the various general principles of third party liability would be engaged when defamation-related claims arise against internet intermediaries.

Article 5 (2) of the UK Defamation Act creates a defence for a website operator that can show that it has not posted the defamatory speech on its site. This can be likened to the conditions governing the availability of the hosting defence in Article 14 (1) ECD, which requires that an intermediary service provider stores information at the request of a service recipient, and that that recipient does not act under the authority of the host.[833] This defence is unavailable when the claimant could not identify the originator of the post and when the claimant provided the website host with a notice and the host failed to respond to that notice.[834] Furthermore, the Act defines the content of a valid notice of complaint and opens up the possibility to specify procedural requirements through separate regulations, such as response times for notices and provisions on dealing with the identity of the originator.[835]

These provisions have been described as making the immunities of the ECD redundant.[836] While the Defamation Act indeed appears to impose conditions that are congruent with Article 14 ECD, it can also be argued that it makes use of the options provided in the ECD for Member States to formulate additional provisions for NTD or for duties of care. The Defamation Act provisions are indeed more detailed than those of the ECD. Regarding duties of care, the fact that the website operator only has a defence if the claimant was able to identify the originator of the defamatory comments (and reacts to notices), may incite the operator to put systems in place that discourage or ban anonymity.[837] Anonymity is to this day one of the major problems of dealing effectively with defamation and

832 Defamation Act 2013 c. 26.
833 Directive 2000/31 (ECD) Article 14 (2).
834 Defamation Act 2013 c. 26 Article 5 (3).
835 ibid Article 5 (5) (6).
836 Kohl (n 280) 192–193.
837 Alex Mills, 'The Law Applicable to Cross-Border Defamation on Social Media: Whose Law Governs Free Speech in "Facebookistan"?' (2015) 7 Journal of Media Law 1, 28.

other unlawful speech acts.[838] However, this defence has apparently rarely, if ever, been used by intermediaries during its more than five years of existence. Website operators may find this provision too complicated and unattractive compared to other available defences.[839]

UK case law shows that courts can rely on several legal sources when determining the liability (exemptions) of intermediaries in defamation cases: ordinary law, represented by common law concepts of innocent dissemination or knowing involvement in publication,[840] the aforementioned Defamation Act and the ECD, as transposed by the 2002 Electronic Commerce Regulations.[841] While in most cases online intermediaries have rarely been found directly liable for defamatory comments, UK judges tend to look first at the common law and nationally based provisions before making use of the EU law.[842]

In *Bunt v Tilley*,[843] the claimant Mr. Bunt brought proceedings against several IAPs alleging they were responsible for defamatory comments made on a blog that was communicated using the IAPs' services. The judge looked first and foremost at the common law defence of innocent dissemination and concluded that the IAPs were entirely passive. This meant they did not need any other defences, such as for example provided by the 1996 Defamation Act or the 2002 Electronic Commerce Regulations.[844] Nevertheless, in examining these statutes the judge found that these additional defences would also have been valid.

Tamiz v Google, decided six years later, deals with defamatory content on a blog hosted by *Google*. The claimant alleged that *Google* was liable for the defamatory comments by failing to remove them in a timely manner. The case was heard by the same judge who sat in *Bunt v Tilley,* and decided using the same methodology, coming to an identical conclusion. *Google* did not act as a publisher according to common law principles and therefore

838 Omer (n 493) 319–320.
839 Wilson Brett, 'Defamation Act 2013: A Summary and Overview Six Years on, Part 2, Sections 4 to 14 –' (*Inforrm's Blog*, 30 January 2020) <https://inforrm.org/2020/01/30/defamation-act-2013-a-summary-and-overview-six-years-on-part-2-sections-4-to-14-brett-wilson-llp/> accessed 13 March 2020.
840 *Bunt v Tilley & Ors* (n 815) paras 17, 23.
841 The Electronic Commerce (EC Directive) Regulations 2002 Articles 17 - 19.
842 Kohl (n 280) 192–193, 197.
843 *Bunt v Tilley & Ors* (n 815).
844 ibid 37.

did not need a defence under the other two statutes.[845] However, it would have been accorded such defences under the 1996 UK Defamation Act and, alternatively, under protections afforded to hosting providers under the 2002 Electronic Commerce Regulations. The appeals court agreed in principle that *Google* would not be a primary or secondary publisher under the common law principle of innocent dissemination. However, for the five weeks that elapsed between notification and removal the company would have associated or made itself responsible for the comments and thus be seen as a publisher.[846] Since the case was struck out because of triviality the court did not see a need to look into the potential availability of immunities under the Electronic Commerce Regulations.

Finally, in the more recent case of *Galloway v Frazer & Others*,[847] a Northern Irish politician brought an action against *YouTube* alleging that the VSP was responsible for publishing defamatory videos about him. *Google* sought the protections of the Article 14 ECD hosting provider immunities for its *YouTube* service. The judge in this case again mentioned the possibility of *Google* to seek protection under common law, the 1996 Defamation Act and the EU-law-based 2002 Electronic Commerce Regulations. Finding that "*while there are striking similarities between these different defences, there are obvious differences*" the court looked first at the common law protections applied in preceding cases.[848] It judged that the reasonable time to react to a notice had been overstepped. 23 days was perceived as too long given the gravity of the allegations. Therefore, the common law concept of knowing interference in the publication applied for the time between notification and removal. The remainder of the judgement seems to indicate consideration of the 1996 Defamation Act, which requires that a website operator must have no knowledge or reason to believe that they contributed to a defamatory publication for it to have a defence. The finding that *Google* did not react swiftly enough given the serious and alarming nature of the comments may also indicate reference to the 2002 Electronic Commerce Regulations, which require an expeditious removal after notification.[849]

---

845 *Tamiz v Google Inc Google UK Ltd* [2012] England and Wales High Court (Queen's Bench Division) HQ11D03178, [2012] EWHC 449 (QB) [39].

846 *Tamiz v Google Inc* [2013] England and Wales Court of Appeal (Civil Division) A2/2012/0691, [2013] EWCA Civ 68 [34–36].

847 *Galloway v Frazer, Google Inc (YouTube) and Ors* (n 627).

848 ibid 67.

849 ibid.

In all three cases the hierarchy and relationships between the available defences are ambiguous. Moreover, the harmonising element of the ECD is not at all visible. The UK judges may, understandably, be more interested in finding the most appropriate and effective provisions to deal with the legal conflict at hand, rather than establish a hierarchy of the available legal defences. If, however, common law doctrines exist in conjunction with national provisions on defamation and the latter include specific provisions for online intermediaries, EU law may indeed be perceived as redundant in litigation practice.[850] This applies even more where the EU law leaves considerable room of interpretation and lies outside of national legal traditions and customs. It should be said that the newer 2013 Defamation Act has alleviated some of this disaccord with the 2002 Electronic Commerce Regulations, which however, appears to be scarcely used in practice.

b. France

In France, the delict of defamation is defined through the 1881 Press Law.[851] This law is used for determining whether a remark or publication qualifies as defamatory. The law is more geared towards responsibilities of press publication in a pre-digital world, as it envisages civil and criminal sanctions mainly against the authors, editors and directors of publication.[852] In 1982, the law on audiovisual communication[853] introduced communication to the public by audiovisual means into the 1881 Press Law, tying responsibilities to the same parties. Finally, when France adopted the ECD through its 2004 *Loi pour la confiance dans l'économie numérique* (LCEN) it extended the rules of the 1982 law to electronic communications. This added the intermediary liability protections[854] to all infractions covered by the French Press law, including defamation, but also incitement to violence, hate and discrimination.

---

850 With Brexit this has now indeed become a mere theoretical point. However, it still serves as a good example of the complex interplay between national and EU intermediary rules.

851 Loi du 29 juillet 1881 sur la liberté de la presse Articles 29 - 35.

852 Renard and Barberis (n 361) 130–133.

853 Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle 1982 Article 93-3.

854 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique 2004 (2004-575) Article 6.

While the main defences of this law target primarily editors and publishers, there is also the more generally available defence of *prescription* which stipulates that a defamatory act can only be complained against within three months after which it was committed. This extends to internet publications and may constitute an additional defence for intermediaries in France. It has been differently interpreted by French courts. Earlier judgements saw internet publications, due to their characteristic of allowing for unlimited re-publications, as constant and successive offences. Consequently, the prescription period of three months started when such publication ceased, which questions the adequacy of this defence for internet publications.[855] Another court stipulated that the prescription period started anew with each modification of an internet address.[856] Finally, later judgements appear to concur that the prescription period starts with first publication, a date which is easily established from the server logs of internet hosts, or at the date when a judicial summons is delivered to the registry of a court.[857]

A glimpse on the interaction between the ordinary law defences on contributory liability in the *Code Civil*[858] and the defences available through French press law, and *inter alia*, the hosting immunities provided by the LCEN, can be gained from the above-mentioned case of *Les Editions R. v Google France.*[859] A claimant brought an action against *Google Search's* autosuggest functionality, which associated his name with the term *escroc ("crook").* First, the court rejected the claims for defamation and public injury according to the Press Law: the action had passed the prescription period of 3 months. Secondly, the autosuggestion function was seen as protected by the freedom to impart and receive information. Thirdly, the court also denied the claimant the parallel application of the *Code Civil* if this concerned an action that the claimant had already targeted by invok-

855 *Carl L v Raphaël M, Thierry M et Réseau Voltaire* (2000) Unreported (Tribunal de Grande Instance de Paris 17ème chambre, Chambre de la presse).

856 *Jean-Louis C v Ministère public, la Ligue internationale contre le racisme et l'antisémitisme (Licra), la Ligue française pour la défense des droits de l'homme et du citoyen, le Mouvement contre le racisme et pour l'amitié entre les peuples (Mrap) et l'Union des étudiants juifs de France (Uejf)* (1999) Unreported (Cour d'appel de Paris 11ème chambre correctionnelle, section A). For this and the judgement in (n. 790) see also : Renard and Barberis (n 361) 131.

857 *Les Editions R v Google France, Google Inc* (2013) Unreported (Tribunal de grande instance de Paris 17ème chambre civile).

858 Code Civil - Articles 1240 & 1241.

859 *Les Editions R. v Google France, Google Inc.* (n 856).

ing the French Press Law. Invoking the *Code Civil* in this way was seen as a means to circumvent the procedural obligations of the French Press Law. Considering that a successful claim for defamation and public injury would have engaged the hosting provider protections of the LCEN/ECD, then it can be argued that the *Code Civil's* contributory liability provisions and the LCEN are mutually exclusive for defamation cases. Meanwhile, a case against *Wikimedia France*, where this association was charged with deleting a Wikipedia page with defamatory remarks, was struck out by the Paris appeals court because the claimants failed to call on the appropriate provisions of the French Press Law. The court reminded the claimants that alleged abuses of the freedom of expression, including against intermediaries, could only be repaired by the 1881 Press Law, and not by the *Code Civil*.[860]

It appears therefore that defamatory acts or any acts sanctioned under the French Press law that involve online intermediaries, would automatically disqualify the (joint) use of the *Civil Code* and the LCEN provisions concerning online intermediaries. Meanwhile "neighbouring" offences such as denigration would allow for the engagement of the LCEN and the Code Civil.[861] For these acts, broader contributory liability rules of the French *Code Civil* and the bespoke online intermediary protections of the LCEN) coexist and are not mutually exclusive but rather apply in a cumulative manner.[862]

c. Germany

In Germany, defamatory acts are covered by Article 323 of the German civil code (BGB),[863] which imposes damage reparation on those who violate the life, body, health, property or other rights of others. The most common unlawful acts committed online that fall under this provision are violations of personality rights, such as defamatory acts, denigration or statements of false facts.[864] It should be noted that the wide formulation of this Article also opens the door to further liabilities. False or inciting state-

860 *Monsieur X et la société Z v Wikimedia France* (2014) Unreported (Cour d'appel de Paris, Pôle 2 – Chambre 7).
861 *M X et Nouvelles de l'annuaire Français v Qwant* (2020) Unreported (Cour d'appel de Paris, pôle 1, chambre 3).
862 Benabou (n 334) 880–881.
863 BGB Article 323 - Schadensersatzpflicht.
864 Hoeren and Bensinger (n 337) 4.

ments may also engage product liabilities or infringe the right to conduct a business. These claims however are usually not directly invoked by claimants.[865] Meanwhile, defamatory comments may also be punishable under the German criminal code. Articles 187 makes libel and slander of defamatory comments punishable with up to 5 years imprisonment. Articles 185 and 186 make "neighbouring" offences such as insult and malicious gossip subject to a maximum of two and one year imprisonment, respectively.[866] In German practice, the *Telemediengesetz (TMG)* which transposes the ECD into German law[867] acts like a filter before any responsibilities according to the civil and penal codes are being allocated.[868] Courts would therefore look first at the qualification of the online intermediary in question as a host or mere conduit and then apply concepts of interferer ("*Störer*") liability in view of the applicable sectoral provision of the unlawful act.

With regards to defamatory comments this means that once qualified as an online intermediary under the *TMG*, German courts apply the interferer liability doctrine. The BGH decided in its *Blogspot* judgement that a *Google*-owned blog portal only needed to fulfil its due diligence obligations once it had been notified of defamatory comments. However, the BGH acknowledged that it may be difficult for a host provider to determine the legal nature of defamatory content. A host provider would only need to act, if the notification was detailed and specific enough in order to affirm its illegality without difficulty, i.e. without detailed legal and factual analysis.[869] Once, however, the illegal nature of the content had been established it had not only an obligation to remove it, but also to prevent future violations of this kind.[870] It should be noted that the relatively formalised procedure to determine and apply interferer liability means that German courts can draw from jurisprudence in other legal areas, such as violations

865 ibid 4–5.
866 Strafgesetzbuch Article 185 - 186.
867 Telemediengesetz Articles 7 - 10.
868 Hoeren and Bensinger (n 337) 19; Spindler, 'Präzisierungen Der Störerhaftung Im Internet Besprechung Des BGH-Urteils „Kinderhochstühle Im Internet"' (n 723) 107. This statement, however, needs to be qualified for copyright infringements, where courts lately tend to establish first whether the intermediary engages in direct violations of copyright, thus sidelining the verification of the hosting provider status.
869 *Verantwortlichkeit eines Hostproviders für einen das Persönlichkeitsrecht verletzenden Blog-Eintrag (Blogspot)* [2011] BGH VI ZR 93/10, GRUR 2012, 311 [25 0 27].
870 ibid 24.

of trademark rights or protection of minors. While this makes for a conceptually unified and predictable approach[871] it has also been criticised as being disproportionate. Applying duty of care *modus operandi* from, for example, the area of economic rights (such as IP) may not take account of the specific balancing exercises needed in the area of online speech.[872] The fear would be that automated infringement prevention technologies e.g. from the area of counterfeit prevention online, be applied directly to the area of defamation, leading to an undue restriction of speech and expression online.

d. Differences in assessing the manifestly illegal nature of defamation

Due to the different normative evaluations of national defamation laws, there are also differences at national level in determining when and if defamatory speech is manifestly illegal. This in turn may have an influence on the presumed knowledge after notification and the expectation of proactive duties according to the diligent economic operator concept.

Austrian courts have repeatedly held that defamatory comments are manifestly illegal and could therefore be more straightforwardly determined by intermediaries following a notification.[873] In the *Facebook* case judged by the CJEU, the Austrian court of first instance explained its preventive injunctions with the argument that the social network had failed to remove clearly obvious unlawful comments after being notified.[874] In the same vein, Belgian courts have ruled incontestable defamatory comments as manifestly illegal.[875]

Meanwhile, German, French, Dutch or UK courts have been less straightforward, with at times contradictory assessments regarding the manifestly illegal nature of defamatory comments.[876] In the *Blogspot* judgement the BGH said that a host provider could not always be expected to identify defamatory comments as clearly unlawful. It would need to rely on specific notifications and statements from involved parties to help it de-

871 Swiss Institute of Comparative Law (n 652) 286.
872 Spindler, 'Präzisierungen Der Störerhaftung Im Internet Besprechung Des BGH-Urteils „Kinderhochstühle Im Internet"' (n 723) 107.
873 European Commission, 'SEC(2011) 1641 Final' (n 11) 34. Van Eecke and Truyens (n 316) Chapter 6 18.
874 *Glawischnig-Piesczek v Facebook*, [2016] Handelsgericht Wien 11 CG 65/16 w - 17.
875 European Commission, 'SEC(2011) 1641 Final' (n 11) 35.
876 Verbiest and others (n 315) 51–61, 100.

cide whether to remove or retain the comments in question.[877] Earlier decisions by German courts have been less indicative on this matter.[878] French courts have also absolved host providers from needing to investigate whether comments posted on *YouTube* against an apparel retailer constituted defamation. In this case, defamation did not necessarily constitute a manifestly unlawful act.[879] By contrast, in the UK *Google* was faulted for failing to identify notified content concerning an MP as clearly defamatory.[880]

The ECtHR has implied in its *Delfi* ruling that defamation constituted clearly unlawful speech, putting it on the same footing with hate speech and incitement to violence. It found that liability of intermediaries for such speech was an effective remedy for protecting the personality rights of the persons targeted by this kind of unlawful speech.[881] The assessment of the clearly unlawful nature of the comments posted on the *Delfi* website played a role when finding the company guilty of failing to remove and prevent this kind of content.

The expectations on online intermediaries to determine the unlawful nature of speech notified to them differ across the EU. On the one hand, it appears excessive to enlist private intermediaries in content decisions that affect fundamental rights, especially when there is no clear-cut case over the nature of the content. Private actors are ill fitted to make decisions that should be reserved to regulators and judges. Today's online platforms are more often than not driven by commercial interests that aim at maximising revenue from online content and that influence content management decisions. On the other hand, in the face of the ongoing flood of unlawful speech on the internet, what choice exists other than involving these essential communication intermediaries more proactively in this fight? This will become even clearer when looking at other, more harmful, types of unlawful content. The ECD has not been helpful in finding a common EU approach to making the intermediary liability exemptions provide an effective remedy for violations of personality rights.

877 *Blogspot* (n 868) paras 25–27.
878 Hoeren and Bensinger (n 337) 29.
879 *H&M Hennes & Mauritz Logistics GBC France et H&M Hennes & Mauritz AB v Google Inc, Youtube* (2013) Unreported (Tribunal de grande instance de Paris).
880 *Galloway v Frazer, Google Inc (YouTube) and Ors* (n 627) para 67.
881 *Delfi* (n 777) para 67.

e. Defamation and the interactive, social web

Before the rise of Web 2.0 intermediation, defamatory acts were almost entirely restricted to postings on newsgroups or bulletin boards that were accessed by other users. Social media, UGC intermediaries and personalised web navigation have added a new dimension to not only defamatory acts but all sorts of unlawful content. The specific challenges of the interactive web with regards to defamation law and intermediary liability shall be briefly lined out.

Search engines have developed Autocomplete or Suggest functions with the aim to accurately predict searches conducted by users. Social networks and UGC platforms direct user attention. They manipulate the dissemination of information through recommender functionalities, targeted filtering or pre-defined personalisation choices of how to engage with content.[882] These functionalities are based on conscious architectural design choices by todays' online intermediaries aimed at maximising attention, amplifying messages selectively and personalising the user experience.[883] This is ultimately done for nothing else than business reasons:[884] Advertising revenue is linked to the ability to optimise microtargeting of users while at the same time maximising the circulation of and exposure to content. Although most of these nudging mechanisms remain opaque and subtle, they are powerful and put in question the role that these platforms play in the publication process.

Would a search engine that suggests an association of a defamatory remark with a specific search term be a mere passive host or actually provide its own content and become liable as a publisher?[885] In Germany, the BGH saw that *Google Search* provided its own content when suggesting additional words in order to complete a users' search. The autocomplete functionality did not qualify as mere conduit, caching or hosting activity.[886] Nevertheless, the BGH chose not to apply direct publisher liability but resorted to *interferer liability*, charging *Google* with failure to apply duties of care that would also apply to a hosting provider after being notified of the search suggestion's unlawful nature. It appears that the BGH took account

882 Lavi (n 199).
883 Oster (n 816) 351. Lavi (n 199) 64.
884 Anupam Chander and Vivek Krishnamurthy, 'The Myth of Platform Neutrality' (2018) 2 Georgetown Law Technology Review 17, 404.
885 Oster (n 816) 359.
886 *Verantwortlichkeit des Betreibers einer Suchmaschine mit Suchwortergänzungsfunktion* [2013] BGH VI ZR 269/12, 108/2013 JurPC WebDok [20].

of the fact that the autocomplete function rested on an algorithm which, while producing the unlawful association, was not intentionally designed to violate the rights of others. However, *Google* would need to take measures to prevent that its software violates the personality rights of others.[887] What appears to be important is that the BGH recognised the active nature of this intermediary service and refused to apply the intermediary liability immunities of the ECD. *Oster*, by contrast, argues that such a function would make search engine providers content owners.[888]

Other nudging mechanisms of social media or UGC platforms mentioned above have scarcely been the subject of intermediary liability considerations as yet. In *Facebook*, the CJEU noted the risk inherent in social networks that *"information which was held to be illegal is subsequently reproduced and shared by another user."* This and the availability of automated search tools and technologies arguably influenced its decision to confirm *Facebook's* proactive duties to prevent the spread of defamatory remarks as adequate. Meanwhile, users that "Like" defamatory remarks on *Facebook* have been found as potentially being liable for defamation. However, *Facebook's* own involvement in providing a medium and the architecture for amplifying defamatory remarks in this way was not discussed in this recent Swiss case.[889] The role of these architectural nudges is more than just neutral: the intermediary facilitates the generation of content that it prefers on its platform. The use of automated content management tools that rely on big data only exacerbates that activity. In that context, a truly neutral design or provision of technical infrastructure may not exist,[890] or may indeed have never existed since the ascendance of Web 2.0. May greater liabilities for (evil) nudges, whose content management practices cause severe harm, be justified?[891]

IV. Summary and outlook

An authoritative, EU wide interpretation of the obligations of online intermediaries in the fight against defamatory speech comes from the CJEU's

887 ibid 26.
888 Oster (n 816) 359.
889 André Müller, 'Wegen Facebook-Likes verurteilt | NZZ' *Neue Zürcher Zeitung* (29 May 2017) <https://www.nzz.ch/zuerich/aktuell/bezirksgericht-zuerich-wegen-facebook-likes-verurteilt-ld.1298231> accessed 24 March 2020.
890 Lavi (n 199) 28–32. Chander and Krishnamurthy (n 883).
891 Lavi (n 199) 71–82.

Facebook ruling. First, it appears that online intermediaries like *Facebook* can safely rely on the hosting provider protections as long as national courts determine it this way. The removal duties after notification remain reasonably clear, yet the decision on the manifestly illegal nature that will stir intermediaries into action lie again with national courts. On the preventive obligations, it appears that a diligent operator in a defamation scenario would need to prevent the identical comment from any user on its network, and similar comments only from the user at fault. The implication is that, following a sufficiently specific and detailed notification, automated tools could be tuned in a way that allow for an effective prevention of the same and similar comments without manual intervention. Manual intervention, on the other hand, would not only be seen as too onerous, but also as coming close to a (prohibited) general monitoring obligation. Whether this provides enough clarity for intermediaries in future defamation cases is open to question. First, the determination of the hosting provider status may be thwarted by other provisions in national defamation laws. Secondly, an active provider may be subject to differing obligations according to national systems, which may not even foresee such a hybrid role (e.g. like France but unlike Germany). Thirdly, the CJEU's *Facebook* guidance on hosting providers duties may still undergo assessment of the various national secondary liability rules. All this makes for rather disparate applications of the intermediary liability rules in the EU with regards to defamatory speech online.

Given its largely private law nature and the national competencies of Member States on defamation, there have been no specific policy actions at EU level. However, given the ongoing salience of the issue a more coordinated policy at EU level may indeed be beneficial for the protection of EU citizens.[892] The border between defamatory remarks, hate speech and incitement to violence is often fluid. In the face of the incessant continuation of defamatory comments, but mainly because of its more extreme iterations, the EU and Member States have stirred into policy action over recent years. At national level notably Germany, France and the UK have passed national laws in the area of hate speech and disinformation that may also cover certain defamatory acts. These shall be treated in the next section in more detail.

892 Savin (n 384) 142.

2. Hate speech

I. The phenomenon of hate speech on Web 2.0

The ever-growing connectivity of people worldwide through social media and UGC platforms did not remain unexploited by extremists and populists. Recent negative events around the world, such as the 2008 financial shock, migrant crises, terrorist attacks, environmental disasters or the Covid 19 pandemic have been widely exploited by these people to spread their extreme views via the internet. The internet allows for the sort of information intermediation that would appear to provide a fertile ground for the spread of extreme, polarising and hateful speech. The sheer scale of publications on the internet makes their identification and categorisation frustratingly cumbersome. Digital publication is instantaneous, global in its reach, notoriously difficult to eradicate and can be multiplied and shared endlessly. Most speech is hosted by a handful of intermediaries which connect "communities" of hundreds of millions, or even billions of users. It is distributed through content management practices that are little understood outside the corporate realm of these intermediary platforms. Speech on these networks is published with virtually no editorial control.[893] Last but not least, hate speech online is facilitated also by the relative ease with which a speaker can obscure their identity and post anonymously.

Hard data on the global spread of hate speech is difficult to come by due its elusive nature and different definitions of the phenomenon at national level. However, various national and regional statistics and reports testify to the rising influence of hate speech online and its negative impact on open and democratic societies. Hate crimes in general are also thought to be widely underreported.[894] This has a lot to do with the fact that the loud-

893 Catherine O'Regan, 'Hate Speech Online: An (Intractable) Contemporary Challenge?' (2018) 71 Current Legal Problems 403, 416–417.

894 Iginio Gagliardone and others, *Countering Online Hate Speech* (UNESCO 2015) 13; Daniel Geschke and others, '#Hass Im Netz - Der schleichende Angriff auf unsere Demokratie' (Institut für Demokratie und Zivilgesellschaft (IDZ) 2019) <http://www.das-nettz.de/publikationen/hass-im-netz-der-schleichende-angriff-auf-unsere-demokratie> accessed 3 April 2020; Laetitia Avia, Karim Amellal and Gil Taïeb, 'Renforcer La Lutte Contre Le Racisme et l'antisémitisme Sur Internet - Rapport à Monsieur Le Premier Ministre' (2018) 10–11 <https://www.gouvernement.fr/rapport-visant-a-renforcer-la-lutte-contre-le-racisme-et-l-antisemitisme-sur-internet> accessed 21 April 2021. 'State of Hate 2020 - Far Right Terror

est, vilest and most extreme speakers usually intimidate those with measured views and respectful and tolerant debating cultures. It also leads to the latter withdrawing from the debate, seemingly leaving the field to the "haters" and extremists and thus causing chilling effects to freedom of speech. In addition, there is a proven link between the spread of hate speech via social networks, on the one hand, and radicalisation of certain parts of society and acts of violence against minorities or certain groups of society, on the other. Its impact is particularly grave and dangerous for young people and minors.[895] Hate speech has become a hotly debated issue for politicians and societies, and, together with fake news, has, according to *Edwards*, become one of the "two new horsemen of the infocalypse"[896] over the last decade.

Despite an almost global recognition of the problem there is no internationally agreed definition of hate speech. The variety of definitions and legal instruments on the subject appear to target most commonly speech that is xenophobic and racist.[897] However, most people today, and indeed many legal instruments, would also include all sorts of speech that discriminates and incites to hatred and violence against people on the basis of their gender, sexual orientation, a disability, age, religion, social, political and other characteristics. Another common characteristic is that hate speech is based on unsubstantiated, distorted or false facts.[898]

Goes Global' (HOPE not hate 2020) <https://www.hopenothate.org.uk/wp-content/uploads/2020/02/state-of-hate-2020-final.pdf> accessed 9 April 2020.

895 Philip Brey, Stéphanie Gauttier and Per-Erik Milam, *Harmful Internet Use. Study Part II, Part II*, (European Parliament, European Parliamentary Research Service 2019) 18 <http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624269/EPRS_STU(2019)624269_EN.pdf> accessed 6 April 2020; Geschke and others (n 893); Avia, Amellal and Taïeb (n 893) 12.

896 Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 286.

897 Alisdair A Gillespie, 'Hate and Harm: The Law on Hate Speech' in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) 490.

898 Savin (n 384) 140.

II. The legal framework of hate speech

a. Fundamental rights at stake

Like in the area of defamation, hate speech online engages different, at times conflicting fundamental rights. On the one side of the spectrum is the right to freedom of expression which is broadly protected both under the CFREU and the ECHR.[899] This covers controversial and borderline speech that may disturb, offend or shock, because its toleration is a necessity for the existence of an open and democratic society.[900] On the other side, incitement to hatred and violence may affect the dignity, equality and safety of the targeted persons.[901] Different legal instruments, that commonly rely on international human rights standards, may spell out these rights in a variety of ways. For the EU, they are guaranteed through the CFREU in Articles 1, 6, 7, 10, or Title III, which, respectively, protect human dignity and guarantee the freedom to security, and private and family life, conscience and religion and equality to everyone. Under the ECHR and the ECtHR case law this may involve for example the protected right to a private life (Article 8)[902] or the prohibition of discrimination (Article 14).[903] It should also be remembered that hate speech itself may have a chilling effect on freedom of speech. Both the CFREU and the ECHR have abuse of rights provisions which may be triggered where the borders of freedom of expression are overstepped.[904]

Under the EU legal and cultural tradition hate speech is therefore always subject to a balancing exercise of various fundamental rights with the right to freedom of expression. Freedom of expression is therefore no absolute right and restrictions to its exercise must be limited to what is strictly necessary for the general interest.[905] In the US, by contrast, freedom of speech enjoys a much more blanket protection and asserts itself more readily over potential violations of privacy, personal integrity and dignity and other rights. This also means that online speech that is prohibited in the EU, or its Member States, may be admissible in the US. An early demonstration of these differences in the scope of freedom of speech online can be seen

899 Articles 11 and 10, respectively
900 *Handyside v The United Kingdom* [1976] ECtHR (Plenary) 5493/72 [49].
901 Gagliardone and others (n 893) 27.
902 *Delfi* (n 777); *MTE* (n 784).
903 *Handyside* (n 899).
904 Such as in *Delfi* (n 777) para 136.
905 CFREU Article 52 (1); ECHR Article 10 (2).

from the famous *Yahoo* case in the US and France which was discussed in Chapter 2.[906]

b. EU regulation

Without going into exhaustive detail on the international framework set up in the fight against hate speech online, some key provisions concerning the EU shall be mentioned briefly. The EU became more actively involved in political initiatives concerning hate speech since the 1990s. The Amsterdam Treaty started a process of gradual expansion of the EU's focus beyond a purely economic union. The 1996 Joint Action to combat racism and xenophobia[907] was a first step to coordinate judicial cooperation and encourage Member States to criminalise hate speech. In the following years the EU Treaties included specific commitments to ensuring equality and combating discrimination. Article 10 TFEU defines the fight against *"discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation"* as an aim when the Union defines and implements its policies. To this end, the EU enacted the 2008 Framework Decision to combat racism and xenophobia by means of criminal law.[908] While this instrument does not specifically address hate speech crimes online, it can be seen as the main existing means of the EU to fight hate speech where it concerns racist and xenophobic expressions. This also reflects a general position that no distinction should be made between on- and offline hate crimes.[909]

Racist and xenophobic speech online is, however, targeted through the 2003 Additional Protocol to the Convention on Cybercrime, whose signature is not obligatory for EU Member States.[910] The main thrust of these instruments is to achieve that Member States criminalise hate crime acts,

---

906 *UEJF and Licra v. Yahoo! Inc. and Yahoo France* (n 358); *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme* (n 360). see Chapter 3

907 Joint Action 96/443/JHA to combat racism and xenophobia 1996 (OJ L185).

908 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law 2008 (OJ L 328).

909 Gillespie, 'Hate and Harm: The Law on Hate Speech' (n 896) 496–497.

910 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems 2003 (European Treaty Series - No189). By the time of writing 24 Member States had signed the Protocol and 17 had ratified it.

apply aggravated and standard minimum penalties, enhance international judicial cooperation, clarify jurisdictional issues and regulate the interaction with fundamental rights. The substantive provisions on hate speech crimes, their definition and enforcement remain in the hands of Member States. The broad definitions of hate speech and the relatively broad discretion given to implementing the Framework Decision means that thresholds for criminalising hate speech vary across Member States.[911]

The ECD is another key tool at EU level, as it attempts to harmonise the liability exemptions of the intermediaries through which hate speech is shared and amplified. As will be shown below, the uneven application of these liability immunities also plays out when looking at the interpretations at national level on how internet intermediaries may be utilised in the fight against hate speech. However, it is important to note that Member States, in line with the exceptions provided by the Treaties, may divert from the country-of-origin principle and restrict an ISSP from another Member State to provide services where public policy objectives, which includes the fight against incitement to hatred, are being impacted.[912] Meanwhile, according to Recital 10 ECD, any EU action must ensure a high level of protection of general interest objectives, in particular the protection of minors and human dignity. The significance of hate speech as a crime that may affect Member States' public interest and the mandate of the EU to act in the fight against hate speech, given the Treaty objectives, give both parties strong reasons to act. The ECD's choice of action in this area are self-regulatory codes of conduct. Article 10 (e) ECD encourages the Commission and Member States to create industry codes of conduct regarding the protection of minors and human dignity.

i. The EU Code of Conduct on illegal hate speech online

In 2016, the European Commission brought major internet companies that operate online platforms to the table, in order to conclude such a self-regulatory agreement. The Code of Conduct on countering illegal hate

911 Teresa Quintel and Carsten Ullrich, 'Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, Related Initiatives and Beyond' in Bilyana Petkova and Tuomas Ojanen (eds), *Fundamental rights protection online: the future regulation of intermediaries* (Edward Elgar Publishing 2020) 204.

912 Directive 2000/31 (ECD) Article 3 (4).

speech online[913] builds on the 2008 Framework Decision. It makes the link between the need for an effective application of criminal laws on hate speech, as envisaged by the Framework Decision, and the necessity of online intermediaries to act expeditiously when notified of unlawful hate speech. The Code was a result of EU actions following the March 2016 terror attacks in Brussels. This also underlines the public policy and security aspects of hate speech spread online.

The internet companies commit to review and remove the majority of illegal hate speech within 24 hours of receipt of a valid notification. The code also encourages the IT companies involved to educate users, provide flagging and reporting tools as well as commit resources aimed at the efficient removal of notified content. The companies also commit to have in place internal rules or community guidelines that prohibit hate speech and to review any notifications first according to these guidelines, and secondly, where necessary, according to national law. This is remarkable as it indeed elevates the internal rules of these companies to quasi law, a status that they may already enjoy more discretely given their massive global reach. However, this confirms a more worrying development of public actors outsourcing the enforcement of the law to private companies, without little or no democratic oversight.[914]

The fundamental rights balancing exercises required under EU law are complex. The exercise is made more complex by the variation in national laws. For one, these kind of content decisions can only be operationalised to a certain extent. It remains then open how accurate these decisions are given the time limit of 24 hours. Whether they result in overblocking is another question, however. A doubt can be raised about whether a soft instrument like this code would really pressure these companies to overblock content and traffic, the lifeblood of their business. Secondly, it is of concern that these decisions are put in the hands of private companies whose content management policies are often deeply rooted in US American and often more Libertarian free speech values[915] that may not fit with Euro-

913 'Code of Conduct on Countering Illegal Hate Speech Online' (n 542). The initial participants YouTube, Facebook, Twitter and Microsoft have since been joined by Instagram, Google+, Dailymotion, Snap and Jeuxvideo.com

914 Article 19, 'Responding to "Hate Speech": Comparative Overview of Six EU Countries' (2018) 14 <https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf> accessed 20 August 2018; Quintel and Ullrich (n 910) 206.

915 Danielle Keats Citron, 'Extremist Speech and Compelled Conformity' (2018) 93 NOTRE DAME LAW REVIEW 43, 3.

pean values. It is likely that in order to avoid the quagmire of ruling on a patchwork of national hate speech laws across the globe, social media platforms apply more uniform standards that escape closer scrutiny.

An EU assessment of the regular transparency reports issued by social media companies as part of the Code of Conduct shows increases in the removal rates of notified content from 28% in 2016 to 72% in 2019 and in the 24-hour turnaround time from 40% to 89%. Meanwhile the amount of notifications has been rising continuously. For example, *Facebook* reported an increase in removed hate speech postings from 3.3 million during the last quarter of 2018 to 4 million in the first quarter of 2019.[916] Other measures that social media companies reportedly improved under the Code include processes for trusted flaggers of hate speech, the involvement of civil society in notifying and determining unlawful content, as well as appeals procedures. This all has led the Commission to claim that the Code has become an industry standard.[917]

The Code stays squarely within the limits of the ECD by trying to formalise ex-post standards of content notification and removal that are mainly focussing on the quantitative aspect of takedowns. No commitment is made to bringing transparency into the decision-making processes of these companies, the appeals procedures or the reporting on decision accuracy. There is also no commitment to actions that would improve the prevention of abusive and unlawful behaviour on these platforms in the first place as the worrying trend of an increase in hate speech online continues despite the existence of the Code. There are by now a number of proposals and projects that look at introducing more proactive responsibilities for the prevention of unlawful activities, which shall be discussed in Chapter 6. The narrative of the Code being a "reactive" industry standard rather fits the ethos of the big internet players, which have traditionally rejected any government intervention that interferes with their operating models.[918]

The Code clearly demonstrates the fix the EU finds itself in with regards to the ECD. The Commission may well be wanting to impose more far reaching responsibilities on online platforms. But the main competencies

916 European Commission, 'Assessment of the Code of Conduct on Hate Speech Online - State of Play (Information Note) - 12522/19' (European Commission 2019).

917 European Commission, 'How the Code of Conduct Helped Countering Illegal Hate Speech Online - Factsheet' (2019).

918 Stephen Kinsella, 'Twitter Cannot Keep Hiding Behind Blanket Anonymity' (*Inforrm's Blog*, 6 April 2020) <https://inforrm.org/2020/04/07/twitter-cannot-keep-hiding-behind-blanket-anonymity-stephen-kinsella/> accessed 9 April 2020.

in this regard lie with Member States. The substantive rules on hate speech, the participation in the Cybercrime Convention's Additional Protocol and the ECD allocate the decisive powers to Member States. Under the ECD, the role of the Commission is restricted to encouraging, together with Member States, the creation of codes of conduct. Meanwhile, the formulation of NTD procedures, the imposition of measures to prevent an infringement (in Article 14 (3)) or the application of duties of care (Recital 48) remain in Member States' hands.

The next, more assertive efforts in the EU's strategy to fight the surge of hate content online were its 2017 Communication and the 2018 Recommendation, both aimed at tackling illegal content online. While broader in their sectoral scope, these instruments allocate particular attention to the fight against hate speech, especially in connection with terrorist content.[919] The Commission mentions the progress made through the Code of Conduct in removing and acting on notified illegal hate speech, but also says that unlawful content, including hate speech, remains a serious problem. These two documents provide the first clearer iterations that advocate for the use of proactive detection and removal measures on the side of platforms in the fight against hate speech, and other types of illegal content. Importantly, the Commission puts forward that proactive and automated detection and removal tools would not automatically lead to the loss of the hosting provider immunities under the ECD (Article 14). Moreover, they could be performed in compliance with the general monitoring prohibitions in Article 15 ECD.[920] The latest assessment report of the Code of Conduct also summarises the proactive and automated detection activities undertaken by *Twitter*, *Facebook* and *YouTube.* For the latter two companies, 65% and 87% of removed unlawful content had been picked up by software. All content identified in this way was allegedly reviewed by humans before being removed.[921] The Communication also mentions that a more aligned approach to fighting unlawful content online, which ties together separate efforts across Member States by content type and type of platform, would be beneficial for the fight against unlawful content in general. Nevertheless, sector specific differences would be appropriate and

919 European Commission, 'COM (2017) 555 Final' (n 69) 20; European Commission, 'C(2018) 1177 Final' (n 8) Recital 4.

920 European Commission, 'C(2018) 1177 Final' (n 8) Recitals 24 - 27.

921 European Commission, 'Assessment of the Code of Conduct on Hate Speech Online - State of Play (Information Note) - 12522/19' (n 915) 6–7.

justified.[922] However, since the Recommendation no further rules specific to the combat of hate speech have been issued at EU level.

ii. The AVMSD and the DSA proposal

In the area of media policy, the EU included video-sharing platforms (VSPs) in the scope of the recently recast Audio-Visual Media Services Directive (AVMSD). VSPs now have an obligation to "*take appropriate measures to protect … the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred.*"[923] In addition, VSPs have to protect minors from programs that could harm their development and prevent programs that contain content the dissemination of which constitutes a criminal offence. This concerns terrorist content, child pornographic material and racist and xenophobic hate covered under the 2008 Framework Decision. It means that VSPs that operate in the EU, such as *YouTube*, *Vimeo*, *DailyMotion* or *Twitch*, but also social media platforms that host video content (e.g. *Facebook, Instagram*) will fall under this Directive.

The AVMSD includes a list of concrete protective measures that VSPs may have to take. These are mainly targeted at users, such as providing clear terms and conditions as to non-permissible content, giving users the opportunity to rate and flag content, providing parental control measures or establishing age verification systems. Which of these measures are appropriate, needs to be determined by the VSP after consideration of the type of content, its potential harm and the type of users and their vulnerabilities as well as by considering the general interest.[924] This, however, would require VSPs to engage in a more detailed risk assessment process as to the specific harms that their business model and content may cause. Such an obligation is a useful step in imposing a degree of responsibility and duty of care on VSPs with regards to the prevention of hate speech content. Member States are required to be in a position to assess the appropriateness of the protective measures taken by VSPs.[925] This can be seen as a useful starting point to establish procedures for accountability of these

922 European Commission, 'COM (2017) 555 Final' (n 69) 5–6.
923 AVMSD 2018/1808 Article 28b (1) (b).
924 ibid Article 28b (3).
925 ibid Article 28b (5).

platforms with regards to the measures taken to protect users from hate speech.

Member States may impose stricter requirements. However, they need to follow the intermediary liability framework of the ECD (Articles 12 – 15). The EU warns in particular against any measures that would be in conflict with the general monitoring prohibition of Article 15 ECD, such as requiring VSPs to install upload filters.[926] It also encourages the use of co-regulation to put in place these protection measures. It tasks the European Regulators Group for Audiovisual Media Services (ERGA) with coordinating these measures as well as providing technical advice on regulatory matters in the area of hate speech. [927]

The AMVSD foresees more concrete and proactive measures for VSPs in protecting users against hate speech than what is currently in place for others types of content at EU level. The involvement of the public sector in assessing and supervising the implementation of measures against hate speech constitutes a new step. But the measures are necessarily limited by the ECD's intermediary liability provisions. They do not contain more formalised NTD procedures or detail on the scope of proactive detection measures for hate speech. In addition, the imposition of anti-hate speech measures for one type of content or platform business model, as opposed to the whole sector, may create further fragmentation of the already dispersed intermediary liability landscape in the EU.

The AVMSD needs to be transposed into Member State laws by September 2020. It will be interesting to see how ERGA, Member States' supervisory authorities and VSPs engage in the setup and assessment of protective measures against hate speech (and other regulated content). The arrangements set out in the AVMSD are a first steps towards a co-regulatory structure, and may well be more fitting to create true industry standards than the purely self-regulatory Code of Conduct on hate speech.

The EU's 2020 DSApackage proposes to place enhanced obligations on intermediary service providers. This would also cover actions against illegal hate speech. While the DSA proposal would not be the appropriate vehicle for aligning national provisions of illegal hate speech, it proposes a set of harmonised obligations for intermediaries that target the fight against hate content, where it is illegal under national law. Very large online platforms (VLOPs), in particular, would have to put in place specific risk management systems to address systemic risks related to illegal content, including

926 ibid Article 28b (3).
927 ibid Article 28b (4), Recital 58.

hate speech.[928] The DSA proposal complements sectoral rules, such as those imposed by the AVMSD. The latter would now persist as *lex specialis* for VSPs under the new horizontal provisions of the proposed DSA.[929] The implementation of these new obligations, which will be touched on again in Chapter 6, would be supported through voluntary codes of conduct. The DSA draft specifically refers to the EU Code of Conduct on illegal hate speech as a basis on which new self-regulatory codes of conduct could be based. While the code would remain voluntary in nature, non-participation of a VLOP, where specifically invited to participate by the Commission, could be counted negatively against the platforms when the fulfilment of its new obligations under the DSA is being evaluated.[930] While the enhanced due diligence obligations of the proposal would bring platforms to take more responsibilities in the fight against illegal hate speech, the choice of continuing to rely on largely self-regulatory measures for their implementation is open to debate. As has been shown, self-regulation has proven to be less effective in bringing in place effective and comparable processes in the fight against illegal hate speech. In addition, these kind of initiatives need to be accommodated by already existing measures at national or sectoral level, as for example, the German *Netzwerkdurchsetzungsgesetz (NetzDG),*[931] discussed below, or the AVMSD.[932]

c. Member States

National differences persist in the legal definition of hate speech, the setup of these offences within the legal system and its enforcement and sanction regimes. The border between other kinds of illegal material, such as defamation or terrorist content, may be fluid and Members States may draw the dividing line differently. They may accord different priorities to acts of hate crime, which is, for example, visible from vastly differing efforts and methodologies to collect data on these offences. Depending on the historical experiences and cultural traditions of countries, they may vary in their focus on crimes against certain minority groups. For example, Islamophobic, Anti-Semitic, right wing extremism or homophobic itera-

928 European Commission DSA proposal (n 10) Recital 57, Articles 26, 27.
929 ibid Recital 9.
930 ibid Recitals 67 - 69.
931 NetzDG.
932 Cole, Etteldorf and Ullrich (2021) (n 548) 193.

tions may be given different levels of priority.[933] There are also marked differences in the way hate speech offences are treated through various provisions of Member States' criminal, civil and administrative laws.[934] Meanwhile, progress on a consistent treatment of hate crimes through legislation as agreed under the 2008 Framework Decision has been slow and uneven.[935] This is not the place for a detailed analysis of hate speech laws across EU Member States. However, a short overview of the situation in the UK, France and Germany shall demonstrate that the national differences are also played out in the way hate speech is tackled in the online environment. Moreover, the inconsistencies in the enforcement of these crimes is exacerbated by the heterogenous understanding and application of online intermediary liability provisions.[936]

i. England and Wales

In the UK, hate speech is mainly regulated through criminal law by the Crime and Disorder Act and the Public Order Act. These Acts target behaviour that abuses or insults people on racial or religious grounds and that stirs up racial hatred and hatred on grounds of religion and sexual orientation.[937] Hate speech is also regulated through several civil law provisions under the Protection from Harassment Act and the Equality Act, which is aimed at protecting users of services or premises as well as employees.[938]

Hate speech via electronic communications and the media is covered by the 2003 Communications Act, with the media regulator OFCOM taking control in this area. This Act punishes the senders of offending communications. On a general basis, the 2002 Electronic Commerce Regulations impose obligations on social media platforms to react to notified hate content along the lines of the EU intermediary liability framework. But unlike the Defamation Act, the Crime and Disorder Act and the Public Order

933 Garland and Chakraborti (n 480) 43–47.
934 Article 19 (n 913).
935 Garland and Chakraborti (n 480) 44.
936 Kyriaki Topidi, 'Words That Hurt (2): National and International Perspectives on Hate Speech Regulation' [2019] SSRN Electronic Journal 29–30 <https://www.ssrn.com/abstract=3488718> accessed 6 April 2020.
937 Crime and Disorder Act 1998 subsections 31, 32; Public Order Act 1986 sections 18, 19, 21, 28 & 29B, C, D, E; O'Regan (n 892) 419.
938 Protection from Harassment Act 1997; Equality Act 2010; Article 19 (n 913) 25.

Act, or any other of the instruments mentioned above, do not contain any specific provisions for website operators or internet intermediaries. The new ambiguities and dynamics of unlawful speech online have primarily focussed on an adaption of enforcement guidelines and, through case law, on actions against the originators of the hateful comments. For example, the Crown Prosecution Service adapted its guidelines on prosecuting cases involving communications sent via social media in 2016 to include more speech crimes. However, the effectiveness of these measures in tackling hate speech online has been questioned.[939] The occurrence of hate crimes via social media has not stopped to grow in the UK. Meanwhile, the murder of MP Jo Cox, during the Brexit campaign, and the 2017 terror attacks in Manchester and London shifted the focus of policy makers eventually towards the responsibilities of social media platforms in this battle.[940]

In 2016, the Malicious Communications (Social Media) Bill was tabled for discussion in the UK Parliament. This instrument sought to oblige social media platforms to prevent and filter threatening speech. It proposed that non-filtered access would only be available for users that had provided proof that they were over 18 years of age. Supervision of this Act would have been allocated to the UK media and telecoms regulator, OFCOM.[941] The Bill contained no cross reference to the liability framework as transposed by the 2002 Electronic Commerce Regulations. However, the Bill fell due to the 2017 General Elections and was not further pursued.

In July 2016, the UK Parliament also announced an inquiry into hate crime and its violent consequences, which included an analysis of the role of social media companies in addressing hate crimes and illegal content online. The subsequent report on abuse, hate and extremism online found that, after taking evidence from *Google*, *Twitter* and *Facebook*, social media platforms were "shamefully far from taking sufficient action to tackle illegal and dangerous content."[942] Apart from failure to remove and prevent

939 Sandra Schmitz and Gavin Robinson, 'Das NetzDG Und Die CPS Guidelines Zur Verfolgung Strafbarer Inhalte In Sozialen Medien', *Recht 4.0 - Innovationen aus den rechtswissenschaftlichen Laboren* (OlWIR Verlag für Wirtschaft, Informatik und Recht 2017) 11–12.

940 ibid 9–12.

941 Parliamentary Counsel, Malicious Communications (Social Media) Bill 2017 [HC Bill 44].

942 House of Commons, Home Affairs Committee, 'Hate Crime: Abuse, Hate and Extremism Online' (2017) Fourteenth Report of Session 2016–17 21 <https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60902.htm> accessed 14 April 2020.

notified hate speech and terrorist content it also found that the companies failed to have adequate processes in place to protect their users from harm caused by this unlawful speech. This included inconsistent and haphazard interpretation and enforcement of their own community standards but also a lack of using technology to proactively tackle hate speech.[943] The Parliamentarians passed several recommendations aimed at making online platforms more accountable for countering hate speech online. They recommended a comprehensive overhaul of the entire regulatory framework on hate speech and extremism in order to make it fit for the realities of the digital age.[944] However, the report does not contain any separate assessment of the ECD liability provisions or how the recommendation would fit into these provisions.

It appears that, like in the area of defamation, the interplay between national and EU-based provisions on intermediary liability and the responsibilities of online intermediaries is not clear. Meanwhile, the concerns over the perceived failure of social media platforms to tackle hate speech online have been incorporated into a more general Online Harms Reduction Regulator (Report) Bill in January 2020.[945] This Bill proposes to task the current regulator OFCOM with developing recommendations that impose statutory duties of care on online platform service operators to prevent harms to users. These duties would relate to a specified list of unlawful acts which includes hate speech and discrimination.[946]

ii. Germany

Hate crimes are pursued under several provisions of the German Criminal Code (*StGB*) that include, but are not limited to, insult, libel, slander, public provocation to commit offences, sedition, coercion, threats and the use of symbols of unconstitutional organisations.[947] The latter prohibits for ex-

943 ibid 23–24.
944 ibid 24.
945 Lord McNally, Online Harms Reduction Regulator (Report) Bill [HL] 2020 [HL Bill 22]. This Bill follows the recommendations of the UK Government's Online Harms White Paper (Great Britain and Department for Culture (n 190)), which is based on proposals developed by the UK Carnegie Trust and Woods and Perrin (n 799).
946 Lord McNally Online Harms Reduction Regulator (Report) Bill [HL] (n 944) Article 2A (4)(c) (d).
947 Geschke and others (n 893) 15.

ample the use of the swastika, and other symbols of the Nazi regime, including the Nazi salute. While many of these offences may be easily identifiable as unlawful, the border to defamatory comments, for which the manifestly illegal character is less obvious, remains fluid.[948] Up until 2018 there were no provisions that dealt specifically with hate speech online. The legal obligations of platforms with regards to hate speech were discharged through the *TMG*, the German law transposing the intermediary liability framework of the ECD. This is supplemented by the interferer liability doctrine, which allocates responsibilities along duties of care and negligence principles to social media intermediaries. According to this, the duties of removal of notified unlawful content are complemented by obligations to prevent the re-upload and sharing of removed content. These measures should be reasonable with regards to their technical and economic feasibility, as well as with regards to their impact on the right to freedom of expression.[949]

However, the proactive duties of internet hosts with regards to hate speech differ according to the business model. According to a recent BGH judgement,[950] internet search engines have less attenuated proactive duties with regards to the prevention of once notified (hate speech) content. The claimants in this case had tried to enjoin *Google* from preventing the display of comments that infringed their personality rights and bring the company to install a word filter to that effect. Search engines had clear duties with regards to manifestly illegal notified content, such as incitement to violence, child pornography, hate speech or clearly defamatory content. Nevertheless, with regards to defamation and hate speech, the border was less clear, especially for search engines. They could not be expected to validate the legality of the comments as they typically lacked the contextual information.[951] Imposing proactive duties of care on the line of social media platforms would endanger the business model of search engine operators and, as a consequence, the usability of the internet.[952] This statement of

948 Bernd Holznagel, 'Das Compliance-System Des Entwurfs Des Netzwerkdurchsetzungsgesetzes' [2017] ZUM 2017 615, 618.

949 *Haftung eines sozialen Netzwerkes für durch Dritte hochgeladene ehrverletzende Inhalte, 11 O 2338/16 UVR* [2017] GRUR-RS 2017 103822 (LG Würzburg) [108–110, 119, 124].

950 *Zur Prüfungspflicht des Betreibers einer Internet-Suchmaschine bei Persönlichkeitsrechtsverletzungen* [2018] BGH VI ZR 489/16, GRUR 2018, 642.

951 ibid 35–37.

952 ibid 34.

the BGH is in itself a glaring proof of the power of commercial intermediaries over the accessibility of information on the internet.[953]

Like elsewhere in Europe, the spread of unlawful hate content became a more pressing problem over the last five years and grew into a matter of public interest. In Germany, this phenomenon was fuelled in the wake of the migration crisis in 2015 and further accentuated in the run-up to the Federal elections in 2017. The German government initiated a national code of conduct with *Facebook*, *Google* and *Twitter* at the end of 2015.[954] This *Task Force against Illegal Hate Speech* contained essentially the same commitments as the EU wide code of conduct one year later. The social media companies committed to remove manifestly illegal, notified content within 24 hours and to invest in dedicated resources (staff, processes). However, the government's monitoring report, published in March 2017, still found that the complaints management and removal processes agreed under the *Task Force* fell short of the original commitments. Two of the three participating networks were still not deleting the majority of illegal content notified to them.[955]

The NetzDG

As a consequence, in June 2017, the German Federal Government brought in a law which codified obligations of social media networks with regards to the removal of unlawful content.[956] The law has become known as the *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act) (*NetzDG*). It was the first national regulatory initiative in Europe aimed at tackling the rise of hate speech on the internet directly.

953 Gerhard Wagner, 'Haftung von Plattformen Für Rechtsverletzungen (Teil 1)' [2020] GRUR 2020 329, 331.

954 Bundesministeriums der Justiz und für Verbraucherschutz, 'Together against Hate Speech - Ways to Tackle Onl Ine Hateful Content Proposed by the Task Force against Illegal Online Hate Speech' (2015)

955 jugendschutz.net, 'Löschung rechtswidriger Hassbeiträge bei Facebook, YouTube und Twitter - Ergebnisse des Monitorings von Beschwerdemechanismen jugendaffiner Dienste' (Bundesministerium für Justiz und Verbraucherschutz, Bundesministerium für Familie, Senioren, Frauen und Jugend 2017) <https://www.fair-im-netz.de/SharedDocs/Downloads/DE/News/Artikel/03142017_Monitoring_jugendschutz.net.pdf?__blob=publicationFile&v=3> accessed 22 September 2020.

956 NetzDG.

The *NetzDG* has since been widely analysed and commented on and shall therefore be discussed only briefly.[957] It applies to all ISSPs that operate profit-oriented platforms, which are set up to share content between users or with the public. In addition, it concerns only those social networks which do not have editorial responsibility for the content shared. Platforms with less than two million registered users in Germany are exempt from the complaints, takedown and reporting obligations imposed under this law.[958] The *NetzDG* defines certain provisions of the German criminal code according to which content is unlawful and therefore actionable by the social media platforms. This includes, amongst others, acts that threaten public order and security, such as incitement to hatred or violence against national, ethnic or religious groups, including sedition, depictions that glorify cruelty, or violence against humans, and severe defamation of religious or ideological organisations.

The law obliges social media platforms to have a complaints management system in place for content that has been notified to them as unlawful.[959] That complaints management system includes processes to deal with notified content. Manifestly illegal content will need to be removed within 24 hours and other unlawful content within seven days of reception (with some exceptions).[960] The staff dealing with complaints, or notices, under the *NetzDG* need to receive training on a regular basis. The operation of the complaints management system needs to be checked on a monthly basis by the company management.[961] The platform may involve co-regulatory institutions (i.e. usually set up by civil society and industry) in the decision-making process on notices. In addition, the social media operators need to publish bi-annual reports on their compliance with the law. These reports must contain, amongst others, data on the amount of complaints, removals, turnaround times, information procedures to notifiers and users

957 Schmitz and Robinson (n 938); Gerald Spindler, 'Internet Intermediary Liability Reloaded' (2017) 8 JIPITEC 166; Wolfgang Schulz, 'Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG', *Personality and Data Protection Rights on the Internet, Forthcoming* (2018) <https://ssrn.com/abstract=3216572> accessed 27 August 2018. Thomas Wischmeyer, '"What Is Illegal Offline Is Also Illegal Online": The German Network Enforcement Act 2017' in Bilyana Petkova and Tuomas Ojanen (eds), *Fundamental rights protection online: the future regulation of intermediaries* (Edward Elgar Publishing 2020).

958 NetzDG para 1 (2).

959 ibid 3.

960 ibid 3 (2).

961 ibid 3 (4).

from whom the content originated, and explain the process and organisation of their complaints management system in Germany.[962]

In essence, the *NetzDG* fixes the non-binding measures previously agreed by the 2015 *Task Force*. It focusses on *ex-post*, reactive content removal procedures for hate postings that violate German law. In its current form, it lays out the procedural detail of obligations that internet hosts have already under the ECD.[963]

The *NetzDG* has been criticised mainly on two grounds: 1) The law outsources the decision-making process over illegal hate speech to private actors and imposes potentially more restrictive national standards on content available worldwide. This could lead an undue restriction of speech worldwide.[964] In addition, private companies may be ill fitted to make decisions on the legality of speech with respect to all fundamental rights involved and in difficult contextual situations.[965] 2) The complexity of the verification process, coupled with tight removal deadlines and the threat of hefty fines would lead to over-blocking of content by social media platforms and an overzealous application of automated content filtering.[966] An argument voiced in contrast is that the regulated platforms have little commercial interest to over-enforce. Overzealous blocking would eventually reduce user traffic, popularity[967] and deprive these platforms of valuable advertising revenue. Secondly, social media networks already regulate speech through their private content policies, which are detached from legal standards and public interests. The new law would help to realign the content policies of social media networks to public interest principles. If society deems social media networks so important that their content removals affect freedom of expression, then they should also be held responsible for the protection of other rights.[968]

---

962 ibid 2.

963 Quintel and Ullrich (n 910) 219.

964 Citron (n 914) 7; 'Germany: Removal of Online Hate Speech in Numbers – Kirsten Gollatz, Martin J Riedl and Jens Pohlmann' (*Inforrm's Blog*, 23 August 2018) <https://inforrm.org/2018/08/24/germany-removal-of-online-hate-speech-in-numbers-kirsten-gollatz-martin-j-riedl-and-jens-pohlmann/> accessed 27 August 2018.

965 Schulz (n 956) 8.

966 'EU Action Needed: German NetzDG Draft Threatens Freedom of Expression' (*EDRi*, 23 May 2017) <https://edri.org/eu-action-needed-german-netzdg-draft-threatens-freedomofexpression/> accessed 27 August 2018.

967 Schmitz and Robinson (n 938) 8.

968 jugendschutz.net, 'Stellungnahme von jugendschutz.net zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken

An analysis of the early transparency reports published in 2018 by *Google (YouTube)*, *Twitter* and *Facebook* show that none of the platforms removed more than 50% of the content notified.[969] Meanwhile, the number of notifications received under the *NetzDG* varied significantly. While *Twitter* and *Google* received each in excess of 250,000 notifications, *Facebook* reported just over 1,000. However, the deletion of manifestly illegal content within 24 hours reached over 95% for *Twitter* and *Google*, and 70% for *Facebook.* A proof of systematic over or under blocking could not be established. Despite the transparency reports, the actual decision-making process on an operational level remains shrouded in anonymity. It is evident from the transparency reports that the networks will increasingly apply automated software proactively - during content upload and through ongoing site monitoring - in order to flag potentially unlawful content for human review.[970] How and to what extent these companies have already moved to fully automated removals is, however, unclear. Indications by *Facebook* show that automated removals take place for hate speech content that receives high risk scores, while in other instances this software flags controversial hate speech for final human review.[971]

Meanwhile, *Facebook* received a fine of EUR 2 million from the German Government (currently under appeal) because of allegedly insufficient reporting and opaque complaints procedures. The over 1,000 complaints reported under the *NetzDG* were in stark contrast to the several millions of hate speech removed under the company's Community Standards.[972]

(NetzDG)' 2–3 <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2017/Downloads/03172017_Stellungnahme_jugendschutz.net_RefE_NetzDG.html> accessed 22 September 2020.

969 Medienanstalt Hamburg/Schleswig-Holstein, 'MA HSH - Auswertung von Transparenzberichten Nach NetzDG' (Medienanstalt Hamburg/Schleswig-Holstein 2019) <https://www.ma-hsh.de/infothek/publikationen/ma-hsh-auswertung-der-transparenzberichte-nach-netzdg.html> accessed 16 April 2020.

970 Google, 'Removals under the Network Enforcement Law – Google Transparency Report' <https://transparencyreport.google.com/netzdg/youtube?hl=en> accessed 16 April 2020.

971 Facebook, 'Community Standards Enforcement Report - Hate Speech' (2019) <https://transparency.facebook.com/community-standards-enforcement#hate-speech> accessed 16 April 2020.

972 'BfJ - Pressemitteilungen -Aktuell- - Bundesamt Für Justiz Erlässt Bußgeldbescheid Gegen Facebook' <https://www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190702.html?nn=3451902> accessed 16 April 2020; Facebook, 'Community Standards Enforcement Report - Hate Speech' (n 970).

In December 2019, the German Government published a bill to fight right wing extremism and hate crimes, which intends to change some provisions of the *NetzDG*. It proposes to oblige social media platforms to report certain types of extreme hate speech to law enforcement authorities.[973] On 1 April 2020, the government announced further changes to the *NetzDG* aimed at making it easier for users to get social networks to disclose the data of hate speech perpetrators.[974] It proposes to introduce mandatory counterclaims procedures and oblige social media networks to provide more detail and comparative data in their transparency reports. Social media companies would also need to report more about the basic features and the scope of automated content removal tools, such as training data used, verification procedures and the extent to which scientific and research communities have assisted in the evaluation process.[975] This small detail of the draft is, however, significant and innovative. It may be a start for achieving more transparency and public scrutiny over the automated tools and decision-making procedures of these platforms. It may also provide a counter-balance to the risk of unchecked state influence on social media platforms.[976] The bill testifies to the unsatisfactory results in some areas of the current *NetzDG*. Extremist and hate speech on the internet are an ongoing phenomenon, which was linked to several right wing and extremist terror attacks in Germany in 2019 and 2020.[977]

The new *NetzDG* would also incorporate the changes demanded by the AVMSD (Articles 28a and 28b) with regards to the risk management activities of video sharing platforms in the fight against extremist and child abuse material.

Despite its potential shortcomings, this a useful step to formulate and codify *ex post*, reactive duties of care and a level of public scrutiny that is probably unique in this area. It could be an important element towards

---

973 Christina Etteldorf, 'Bill to Combat Right-Wing Extremism and Hate Crime' [2020] iris Newlsetter <http://merlin-int.obs.coe.int/article/8802> accessed 16 April 2020; Bundesministerium für Justiz und Verbraucherschutz, Entwurf für ein Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität 2019.

974 Bundesministerium für Justiz und Verbraucherschutz, Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes 2020.

975 ibid Article 2 (2).

976 Human Rights Watch, 'Germany: Flawed Social Media Law' (*Human Rights Watch*, 14 February 2018) <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law> accessed 16 April 2020.

977 Such as the murder of district commissioner Walter Lübcke on 2 June 2019, and extremist terror attacks in Halle (2019) and Hanau (2020).

building more comprehensive and transparent risk management obligations for online platforms in the fight against unlawful content.

iii. France

France regulates the substantial provisions on hate speech through the French Press Law of 1881 and the criminal code (*Code Pénal*) . The 1881 Press Law's Article 24 makes incitement to hatred and violence based on a person or group's ethnic, racial or religious characteristics a criminal offence. This text was amended in 1990 by adding Article 24 *bis* and Article 32, which make the denial of crimes against humanity, such as the holocaust, a criminal offence.[978] The criminal code punishes similar hate speech acts when committed through private communications, which also applies to electronic communications. The respective passage of the criminal code was amended several times over the last 20 years in order to increase the scope and penalties for racist acts. In addition, the dissemination of images linked to criminal acts was also made punishable with maximum five years imprisonment and a fine of EUR 75,000, thus adapting it to better target acts of cyberbullying and harassment.[979] This arsenal is completed by the LCEN, which transposes the ECD into French Law.

The French Press Law and the criminal code punish the originators or publishers of hate speech acts. The normative differences to other jurisdictions and the impact on expression on the internet have been vividly demonstrated in the *Yahoo* case described above.[980] Within France, the application of hate speech provisions has also not gone without problems: striking the balance between freedom of expression and hate speech, and the more procedural aspects, that may be less adapted to the online environment, are cases in point.[981] The intricate procedural requirements of the French Press Law and its interplay with the LCEN were already described in the section on defamation. This also applies to hate speech acts.

---

978 Topidi (n 935) 16; Christiane Féral-Schuhl, *Cyberdroit 2018/19 - 7e ed.: Le droit à l'épreuve de l'internet* (Edition 2018-2019, Dalloz 2018) chs 713-Atteintes aux libertés individuelles713.122. Textes.

979 Code pénal Articles 222-33, 222-33-2, 222-33-3, 227-24; Féral-Schuhl (n 977) chs 713-Atteintes aux libertés individuelles713.122. Textes. Agnès Granchet, 'Réseaux sociaux, médias en ligne et partage de contenus : le temps de la responsabilité et de la régulation' [2020] Legipresse 93.

980 See Chapter 3

981 Topidi (n 935) 15.

Like elsewhere in Europe, France has witnessed a surge of hate speech promulgated through social media.[982] The successive attempts to amend the substantive provisions of hate speech laws may be one indication of the continuous efforts of the law maker in that respect. Court cases involving intermediaries have focussed on the obligations of host providers. For example, *Twitter* was found guilty as a host provider under the LCEN of not providing an easily visible and accessible system of notification of unlawful content to its users and for failing to communicate data of users that had posted anti-Semitic content.[983] The courts also confirmed that hosting providers only needed to remove notified content that was manifestly illegal without waiting for a court or authority. Manifestly illegal content was defined as child pornographic material, denial of crimes against humanity and incitement to racial hatred.[984]

A series of grave extremist terror attacks since 2015 brought the role of social media platforms in the incitement to extremist violence and hatred increasingly into the public debate.[985] In 2018, the MP *Laetitia Avia*, published a report aimed at stepping up efforts to combat racism and anti-Semitism on the internet.[986] The report proposed new obligations on social media platforms to remove hate speech. The proposal takes the German *NetzDG* and notably its 24-hour removal target for manifestly illegal hate speech as well as its steep sanctions as an example.[987] On 20 March 2019, *Laetitia Avia* and a number of other Parliamentarians introduced a bill to combat hate content on the internet to the National Assembly (the *Loi Avia*).[988] The bill was adopted into law after a second reading by the *Sénat*, the French upper house of Parliament, on 28 February 2020. By inserting a new Article (Article 6.2.) into the LCEN, social media platforms would be obliged to remove or make inaccessible, manifestly illegal content notified to them. The law defines manifestly illegal content, by referring to specific provisions in the 1881 French Press Law and the criminal

982 Avia, Amellal and Taïeb (n 893) 12–13.
983 *L'Union des Etudiants Juifs de France (UEJF) v Twitter* (2013) (Unreported) (Cour d'appel de Paris Pôle 1, chambre 5). The action in thsi case was based on the LCEN in conjunction with civil procedural rules.
984 *Rose B v JFG Networks* (2013) (Unreported) (Cour d'appel de Paris Pôle 1, chambre 2).
985 Avia, Amellal and Taïeb (n 893).
986 ibid.
987 ibid 5, 20–22.
988 Laetitia Avia Proposition de loi visant à lutter contre la haine sur internet (n 651).

code.[989] Like the *NetzDG*, the manifestly illegal content includes terrorist propaganda and the dissemination of child pornographic material along hate speech. The law introduces a new delict of non-removal of notified content. The maximum fine for platforms that are in contravention of the new law is EUR20 million, or 4% of global turnover, whichever is the higher amount.[990] The bill does not define any exemptions or thresholds for the application of the law, but asks the *Conseil d'État*, the French Government's legal advisory body, to determine such thresholds by decree.

The law obliged platforms, amongst others, to withdraw all terrorist and child pornographic content notified by authorities within one hour. Platforms would also need to withdraw any manifestly illegal content notified by other persons within 24 hours.[991] Other procedural obligations include the provision of standardised and easily accessible notification systems for unlawful content. Platforms need to acknowledge the receipt of a notification, confirm the date and time of the receipt, inform the notifiers of the course of action taken and the reasons behind any decision, such as removal or no action. Content uploaders shall be informed of any removal, the reasons for it and the possibilities of contesting the decisions. They shall also be given a warning that the publication of manifestly illegal content is subject to civil and criminal sanctions.[992] Abusive notifications would be punishable with up to one year of imprisonment and a fine of EUR15,000.[993]

The *Conseil supérieur de l'audiovisuel (CSA)*, France's audio-visual media regulator is given powers to oversee the reporting obligations of platforms, the administration of fines and to coordinate best practice sharing, and cooperation between social media platforms.[994] In the area of preventive measures, the efforts focus on education about the issue of hate speech online. But the law also foresaw the creation of an observatory on online hate speech under the aegis of the *CSA*. This observatory should unite civil society, researchers, social media platforms and administrators to monitor and discuss emerging issues in hate speech online and preventive efforts.[995]

It is true that the French bill was similar to the *NetzDG* in that it focussed mainly on procedural, *ex-post* measures of notices and takedown.

989 ibid Article 1 (II).
990 ibid Article 4 (I).
991 ibid Article 1 (I, II).
992 ibid Article 2 (II).
993 ibid Article 1 (II).
994 ibid Article 4.
995 ibid Article 7.

However, there are some important differences. By charging the *CSA* with overseeing and developing transparency reporting procedures, corrective actions, sanctions and with leading wider cooperation efforts between stakeholders and industry in the fight against hate speech, the proposal goes more in the direction of co-regulation than the *NetzDG*.

The CSA has already been tasked with a similar mandate in the recently passed law against disinformation online.[996] It is also the regulator responsible for implementation of the AVMSD, which now covers VSPs. France appears to put the CSA at the heart of a future co-regulatory system aimed at establishing transversal principles of content regulation on online platforms, and applying them in a differentiated way to the various content sectors and platform operating models.[997]

In May 2020, 60 French Senators brought a challenge to this law in front of France's Constitutional Council, the *Conseil Constitutionnel*. They complained that, notably the one hour and 24 hour withdrawal obligations and the severity of fines imposed contravened several provisions of the ECD, such as Article 3 on the freedom to provide services and Articles 14 and 15 on the liabilities of online intermediaries. They also violated the fundamental rights of freedom of expression and to receive information.[998] On 18 June 2020, the *Conseil Constitutionnel* vindicated the concerns of the Senators by declaring large parts of the law unconstitutional and in contravention of, amongst others, the ECD and its French implementation, the LCEN.[999] The short reaction times accorded to platforms did not take account of the legal complexities related to the legality of certain content and the amount of notifications that platforms receive. Combined with the threat of high fines, this would incite platforms to withdraw content without due consideration, thus impacting freedom of expression and information. In its current form, only two substantial provisions have been retained: Article 2, which spells out the detail of the content and format of a

996 LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information 2018 (2018-1202) Articles 11 & 12.

997 Roch-Olivier Maistre, 'Point d'étape Vers Un Nouveau Modèle de Régulation Des Plateformes' [2019] Legipresse 459.

998 Groupe Les Republicains, 'Saisine CC – PPL Avia lutte contre les contenus haineux sur internet' <https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020801dc/2020801dc_saisine.pdf>.

999 *Décision n° 2020-801 DC du 18 juin 2020, Loi visant à lutter contre les contenus haineux sur internet* [2020] Conseil Constitutionnel 2020-801.

notice, and Article 16, which nominates the *CSA* as the body to host and supervise the creation of the observatory for online hate speech.[1000]

III. Private regulation of hate speech

Social media platforms and UGC platforms have been constantly refining the enforcement of their own content standards or community policies. This is in their own interest. The maximum of (profitable) content engagement can only be achieved when abusive, extreme and illegal behaviour does not put off too many users. Meanwhile, removing too much content may dent user trust and advertising revenue.[1001] From an economic perspective, platforms may only have an interest to remove those kinds of extreme content that lead to a net loss in user traffic and "behavioural surplus."[1002]

Each platform may have its own balance and policy approach depending on the market and the operational model that it has carved out for itself. Consequently, some of them may be more prone than others to attracting and amplifying extreme speech, including hate comments that stray into unlawful territory.[1003] What all of these profit-orientated social media and UGC platforms have in common is that the revenue is highest when the information platform meets the expectations of a maximum of users.[1004] This is the case when the content hits the nerve of the user, leading to increased sharing with like-minded people on the platform and prolonged engagement in front of the screen. That "hitting the nerve" and the occasional virality of a piece of content happen all too often when fringe or more extreme news and opinions are voiced that outrage and confirm own opinions and views.[1005]

The content management practices and policies of platforms are ultimately geared towards the mechanisms that generate additional financial revenue. The community policies and the algorithms that govern the cre-

---

1000 LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet | Legifrance 2020 (2020-766).

1001 Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1599, 1627–1628.

1002 Zuboff (n 5) l 2053.

1003 For a detailed analysis of how this manifests itself in platform architecture and content moderation policies see: Lavi (n 199).

1004 Klonick (n 1000) 1627.

1005 Chander and Krishnamurthy (n 883) 404.

ation and spreading (or not) of content are designed in order to create an environment conducive to advertisers. The right type of content is that which draws a maximum of user attention and which corresponds to the desired target audience of advertisers on a given social network or a section thereof.[1006] Corporate and ethical values and respect of the law may also influence the formulation of content policies.[1007] However, the real weight of ethical and normative corporate values and their application in day-to-day content management is open to debate.[1008]

It is increasingly uncontested that the content management policies of a small number of dominant platforms, which reach hundreds of millions and even billions of people worldwide, create a private regulatory regime for online speech with little accountability.[1009] With regards to hate speech, it may be a challenge for a globally operating network on the internet to respect and comply with the patchwork of different national standards and values, especially since each piece of content is accessible globally. These platforms are under constant pressure to operationalise content management policies on the one hand, and reacting to increasing pressures from regulators to enforce national hate speech standards on the other. A social network platform would try to balance the legal risk of non-compliance in certain jurisdictions against the efficiency loss incurred through adapting global operating procedures to national specificities, while safeguarding its revenue generation. This does not bode well for open and transparent content management practices, and may be harmful to wider public interests where these platforms are gatekeepers of internet content. Companies like *Facebook* or *Google* have, arguably, become more important as actors in regulating content and expression than states.[1010]

Social media platforms want to keep regulators and civil society organisations at bay and prefer self-regulating. Any fundamental debate about

---

1006 Fernando Bermejo, 'Online Advertising as a Shaper of Public Communication' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) 131 <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020.

1007 Which are also called Community Standards (Facebook), Content Policies (Reddit) , Community Policy (LinkedIn), Terms of Service (Google) or Rules and Policies (Twitter)

1008 Zuboff (n 5) l 2056; Citron (n 914) 6–8. Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' (n 83) 233–234.

1009 Wagner, *Global Free Expression - Governing the Boundaries of Internet Content* (n 136) 54.

1010 ibid 116.

the transparency of enforcement processes, the values and risks underlying certain business practices and architectures, such as live-streaming, content amplification algorithms or targeted advertisement may backfire on revenue. This is also meant to obscure the fact that content moderation, by these self-professed passive platforms, is an active selection process of what is and what is not publicly available to users. Reams of borderline and straightforwardly illegal texts, images and videos need to be reviewed, judged, and then removed or allowed by armies of content moderation workers across the globe, or as is increasingly the case, by automated software.[1011]

Social media platforms have reacted to the growing volume and diversity of content online and the mounting pressure of regulators in two ways.

First, they have changed their content policies and the internal content moderation guidelines with increasing frequency.[1012] Content policies are adapted to public opinion, or following user trends, and less strictly enforced if it involves commercially more valuable content types or service recipients. With the overarching objective to derive money from content, the enforcement of these policies is therefore often inconsistent, or even contradictory, if seen from a legal and ethical standpoint. Essential standards of transparency and accountability succumb to changing internal enforcement priorities that are dictated by financial preoccupations.[1013] Secondly, regulatory initiatives are pre-empted by commitments to deploy more staff, build internal oversight boards and use automated removal tools and artificial intelligence.[1014] This may speed up certain removal processes of hate speech and unlawful content, but also make the content management policies even more opaque.

1011 Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018) 120–125.

1012 Klonick (n 1000) 1639.

1013 Sarah T Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (Yale University Press 2019) 95–104.

1014 MacKenzie F Common, 'Fear the Reaper: How Content Moderation Rules Are Enforced on Social Media' [2020] International Review of Law, Computers & Technology 1, 11. Robert Gorwa, 'As Platforms Rely Less on Human Content Moderators, What's at Stake?' (*Centre for International Governance Innovation*, 31 March 2020) <https://www.cigionline.org/articles/platforms-rely-less-human-content-moderators-whats-stake> accessed 22 April 2020; Richard Waters, 'Facebook's Attempt to Prove Impartiality Looks Doomed to Failure' *Financial Times* (22 August 2019)

In parallel to that, there is a determined move to employ fully automated systems that proactively identify and remove unlawful hate speech. This has been demonstrated in the sections on the EU Code of Conduct on hate speech and the *NetzDG*. This proactivity may serve online platforms as a pacifier to regulators, which seek to impose enhanced responsibilities and obligations on platform. On the other hand, these internal content management tools pre-empt more profound investigations and verifications from outside parties as to the standards applied when deciding which content can stay up and which needs to be taken down. The sheer number of automated takedowns and the technical nature of these processes make it difficult to retrace content decisions by platforms without having access to data. The additional benefit for platforms is that these tools can easily incorporate but also mask the frequent changes in content policies and their internal enforcement. Public authorities are placed in the dilemma between welcoming what might appear as a helping hand in enforcing the law, on the one hand, and seeing the actual decision-making process over removals of hate speech moving beyond their sphere of influence, on the other. Meanwhile, the discrepancy between the relatively few notifications received though notifiers and the huge number of automated removals confirms the tendency of online platforms acting as largely unsupervised private regulators of speech and information on the internet that are in direct competition with nation states.[1015]

IV. Summary and outlook

Given the influence of social media platforms as speech regulators, national governments and the EU have first tried to get these companies to enforce their own content policies consistently and transparently. This was mainly attempted through codes of conduct. At a second level, the adherence to national standards, already fixed into law, has been adapted to the specificities of the internet, e.g. in France, Germany and the UK. These efforts are a good start to achieve a more effective and transparent removal of

1015 Mariarosaria Taddeo and Luciano Floridi, 'The Debate on the Moral Responsibilities of Online Service Providers' (2016) 22 Science and Engineering Ethics 1575, 1593; Uta Kohl and Carrie Fox, 'Introduction: Internet Governance and the Resilience of the Nation State' in Uta Kohl (ed), *The Net and the Nation State Multidisciplinary Perspectives on Internet Governance* (2017) 12–14; Belli and Sappa (n 42) 189–190.

notified unlawful content. However, they will arguably do little in bringing more light into risky content management practices that are responsible for the ongoing massive availability of hate speech online in the first place. While at least in Germany, there is no conclusive evidence of systematic over or under blocking following the *NetzDG*, it cannot be denied that these kind of systems continue to outsource the complex enforcement of fundamental rights to private actors. The current efforts may therefore not be enough to ensure accountability for content management decisions that affect freedom of expression, human dignity and democratic order.

The crux is that social media platforms are not responsible as editors for content and can generally claim immunity under the ECD's intermediary liability conditions. Consequently, only reactive procedural duties, NTD or information and transparency requirements, have been imposed on these companies under the national laws mentioned above. But, as has been demonstrated, the new mechanisms of social media clearly give these actors more than just a merely technical and passive role in the information intermediation process.

Rather than just regulating *ex post* mechanisms or curtailing the market imbalances or dominance of certain social media platforms, harmful content management and business practices need to be regulated more systematically. Platform business models and design choices for algorithms and nudging systems that promote or amplify hate speech and other harms need to be openly assessed from a moral and ethical public interest standpoint.[1016] This, however, means imposing prospective obligations along more systemic content governance and risk management mechanisms, which the current legal framework of the ECD prohibits.

The UK appears to incorporate more holistic prospective and retrospective responsibilities of platforms regarding hate speech into the wider reform of online platform responsibilities under the Online Harms Reduction Regulator (Report) Bill. These efforts will ultimately be pursued outside of the EU jurisdiction over the coming years.

France has chosen to task the *CSA* with oversight of both *ex-post* content removal and transparency obligations, as well as more forward-looking societal research, dialogue and best practice sharing in the fight against hate speech online. The *CSA* appears to emerge as a central platform (co-)regulator with competencies that might eventually extend towards establishing

1016 Karine Favro and Célia Zolynski, 'De la régulation des contenus haineux à la régulation des contenus (illicites)' [2019] Legipresse 461. Woods, 'The Duty of Care in the Online Harms White Paper' (n 794).

more forward-looking risk management obligations on platforms in the fight against hate speech and other types of unlawful content. Too onerous *ex-post* withdrawal obligations are clearly out of place. But whether this remains relevant in the context of the automated proactive content removal systems deployed by most large platforms remains to be seen. The new responsibilities of the *CSA* are one of the few parts that were left intact after the *Conseil Constitutionnel* struck down most other provisions of the *Loi Avia*.

Germany intends to toughen the *ex-post* procedural and transparency obligations of social media networks with its new *NetzDG*. Like France, it also wants to shed more light on the mechanisms that govern the identification and removal of hate speech. However, the institutional regulatory structure to support this is less defined and less holistic.

Both approaches are likely to provide valuable insights for a future regulatory framework at EU level for content moderation and intermediary responsibility as envisaged by the European Commission under the future Digital Services Act.[1017] So far, the European Commission has not attempted to tackle the issue of hate speech online through legislation. It remains to be seen whether and how the future DSA would address this particular issue in its final version. The current proposal contains useful, enhanced obligations that would also apply to the removal and prevention of illegal hate speech. It remains, however, questionable whether the choice of accompanying the enhanced obligations with, so far ineffective industry self-regulation may bring the results hoped for. Meanwhile, the decision of the *Conseil Constitutionnel* on the *Loi Avia* should be a warning shot over the red lines that EU lawmakers need to navigate when they draft the DSA.[1018]

1017 'Digital-Services-Act-Note-DG-Connect-June-2019.Pdf' (n 546).

1018 Jean-Sébastien Mariez and Laura Godfrin, 'Censure de La « loi Avia » Par Le Conseil Constitutionnel : Un Fil Rouge Pour Les Législateurs Français et Européens ?' [2020] Dalloz actualité 29 juin 2020.

3. Terrorist content

I. Background

Over 370 people were killed in the EU by terrorist attacks between 2010 and 2018.[1019] Besides of this invaluable human loss, the negative impact of terrorism on the EU's GDP is estimated at EUR180 billion between 2004 and 2016.[1020] In the long term, terrorism, poses a substantial threat to the values of democratic societies and the freedoms, rights and security of its citizens.[1021]

Terrorist groups have early caught on to the opportunities of the internet and digital communications and exploited them to their advantage. The internet already played a key role in the preparation of the 9/11 terror attacks in New York.[1022] In many ways the internet, with its global reach, ease of access, low degree of regulation, increasing means of free encryption, and above all, its anonymity, has become an ideal medium for terrorist purposes. With the emergence of Web 2.0 and social media, the use of the internet by terrorists has expanded even more.[1023] Apart from the logistical coordination of attacks, the internet is used for: psychological warfare and propaganda, by subtle and manipulative communication through social media; for recruitment and mobilisation, including through closed groups and on social media platforms; data mining and virtual training; and for financing. Online fund-raising activities include the soliciting of donations, the sale of drugs, counterfeits or other illegal goods through the Darknet and e-commerce marketplaces.[1024] The European Commission has estimated in 2017 that approximately 10,500 hosting providers were established in Europe, and another 10,000 in the US and Canada that targeted

---

1019 Wouter van Ballegooij and Piotr Bakowski, *The Cost of Non-Europe in the Fight against Terrorism: Study* (European Parliament, European Parliamentary Research Service 2018) vii–ix; European Union Agency for Law Enforcement Cooperation, *European Union Terrorism Situation and Trend Report 2019*. (2019) 8. a combination of European Parliament and Europol data.

1020 Ballegooij and Bakowski (n 1018) vii–ix.

1021 European Council, 'European Counter-Terrorism Strategy - 14469/4/05 REV 4' (2005) para 1.

1022 Allison Miller and Yannis A Stivachtis, 'Investigations of Terrorist Cases Involving the Internet' in John R Vacca (ed), *Online terrorist propaganda, recruitment and radicalization* (2020) 172.

1023 Gabriel Weimann, *Terrorism in Cyberspace: The next Generation* (Woodrow Wilson Center Press 2015) 27–29.

1024 ibid 29–39.

EU users. 150 of these hosting providers were abused for terrorist propaganda. Other reports show 400 platforms being used by *Daesh* for terrorist crimes.[1025] Thanks to the internet, terrorist organisations could expand their international networks substantially. International cooperation on a judicial as well as institutional level is therefore of key importance to effectively combat terrorism.

II. Legal framework against terrorism online – EU and Member States

Due to its effect on national security the fight against terrorism is primarily within the competency of Member States in the EU.[1026] The definition of terrorist offences are therefore down to national law. On a global international level, however, agreement over the definition of terrorism and the scope of terrorist crimes differ. Similar to hate speech, the view on what is extremist and terrorist content may vary, depending on cultural, geographic, historic, temporal and subjective influences.[1027] These differences play out at the political level: one man's terrorist may be another's freedom fighter.[1028] It is therefore no surprise that the UN has as yet failed to come to a consensus definition of terrorism and terrorist entities.[1029] Notwithstanding these differences, there is some consensus amongst liberal democracies over how to define terrorist actors and terrorist offences.[1030] The EU adopted a common position on what it considers terrorist persons and en-

1025 European Commission, 'Commission Staff Working Document - Impact Assessment - Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online - SWD(2018) 408 Final' (European Commission 2018) 6–8.

1026 Treaty on European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2016) Article 4 (2). Allocates Member States with sole responsibility for national security issues.

1027 Donald Holbrook, 'Designing and Applying an "Extremist Media Index"' (2015) 9 Perspectives on Terrorism 57, 58. For more detail: Bruce Hoffman, *Inside Terrorism* (Columbia University Press 2017) 1–44 <https://columbia.degruyter.com/view/title/541544> accessed 23 September 2020.

1028 Boaz Ganor, 'Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?' (2002) 3 Police Practice and Research 287, 290–295.

1029 Chris Meserole and Daniel Byman, 'Terrorist Definitions and Designations Lists - What Technology Companies Need to Know' [2019] Royal United Services Institute for Defence and Security Studies 4.

1030 ibid 4–5.

tities, and terrorist acts.[1031] It has produced a list of terrorist entities and persons that are subject to restrictive measures, which covers mainly the freezing of funds and financial assets and special police and judicial cooperation.[1032] This list is updated every six months.[1033] The 2017 EU Terrorism Directive provides a minimum list of offences that Member States need to define as terrorist crimes under their national laws.[1034] This section will be based on this common understanding of terrorist acts and actors as developed through EU law and agreements reached by the Council of Europe.[1035] It shall, however, be kept in mind that for globally operating online platforms the varying legal interpretations and terrorist entity definitions across the world complicate the task of identification and removal of such content.

Terrorist content and hate speech are often treated closely together, at least where these crimes are committed via the internet. For example, the EU Code of Conduct on Illegal hate speech[1036] makes a link to terrorist acts and propaganda. The *NetzDG* and the *Loi Avia* both include terrorist crimes, such as incitements to terrorist acts or terrorist propaganda within their scope.[1037] Unlike defamation, and, to a lesser extent, hate speech, terrorist content is usually more *prima facie* illegal. *Holbrook*, for example, establishes an extremist media index according to which terrorist iterations would fall under extremist speech that openly supports and incites political violence.[1038] Further clarity would be gained where these iterations are made by social media users that identify with or are linked to designated terrorist entities.[1039]

1031 Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism 2001 (OJ L 344) Article 1 (2, 3).

1032 ibid Articles 2 - 4.

1033 For the latest update at the time of writing: Council Decision (CFSP) 2020/1132 of 30 July 2020 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism 2020 (OJ L 247).

1034 Directive (EU) 2017/541 on combating terrorism 2017 (OJ L 88) Articles 3 - 12.

1035 Council of Europe - Convention on Cybercrime 2001; Council of Europe - Convention on the Prevention of Terrorism 2005.

1036 'Code of Conduct on Countering Illegal Hate Speech Online' (n 542).

1037 NetzDG Article 1 (3). covers as illegal acts linked to terrorist crimes under the German Criminal Code (Articles 89a, 90, 129a, 129b), Laetitia Avia Proposition de loi visant à lutter contre la haine sur internet (n 651) Article 1 (II). refers to the French Criminal Code Article 421-2-5

1038 Holbrook (n 1026) 58–60.

1039 Meserole and Byman (n 1028) 3.

Member States have densified anti-terrorist legislation over the last thirty years, especially where it involves internet and communications systems. France, for example, has continuously adapted its criminal laws by creating new terrorist offenses or raising penalties in line with successive terror attacks. It included terrorist propaganda committed via the internet in its criminal code, and regular user visits to jihadist websites to its Domestic Security Code.[1040] A series of anti-terrorist laws on cybersecurity have imposed data retention obligations on telecommunications operators and IAPs, or given authorities enlarged surveillance powers to collect, monitor and intercept communications data.[1041]

The UK has also continuously adapted its counter-terrorism legislation by making successive changes to the Public Order Act and the Terrorism Act. The scope of terrorist offences has gradually been widened and surveillance, search and censorship powers were stepped up.[1042] The UK Terrorism Act, for example, introduced police powers to request that electronic service providers withdraw terrorist material directly within two working days, bypassing judicial oversight. However, that provision has been virtually unused due to existing informal and voluntary cooperation between law enforcement and social media platforms in this particular area of content, mainly through the Counter Terrorism Internet Referral Unit (CTIRU) set up by the police.[1043] Nevertheless, this demonstrates the potential indirect coercive power of statutory measures that aim at enforcing national security objectives. The CTIRU, set up in 2010, aims to identify terrorist content regulated under the 2000 and 2006 Terrorism Acts. It refers or notifies these pieces of content to online service providers for removal.[1044] It should be noted that these referrals are not equal to official

1040 Céline Castets-Renard, 'Online Surveillance in the Fight Against Terrorism in France' in Tatiana-Eleni Synodinou and others (eds), *EU internet law: regulation and enforcement* (Springer Berlin Heidelberg 2017) 388–389.

1041 ibid.

1042 Thomas J Holt, Joshua D Freilich and Steven M Chermak, 'Legislation Specifically Targeting the Use of the Internet to Recruit Terrorists' in John R Vacca (ed), *Online terrorist propaganda, recruitment and radicalization* (2020) 131; Clive Walker and Maura Conway, 'Online Terrorism and Online Laws' (2015) 8 Dynamics of Asymmetric Conflict 156, 163–166.

1043 UK Parliament, 'Lords Hansard Text for 23 Sep 2013 (Pt 0001)' (2013) <https://publications.parliament.uk/pa/ld201314/ldhansrd/text/130923w0001.htm#wa_st_3> accessed 27 April 2020.

1044 'Counter-Terrorism:Written Question - 30893' (*UK Parliament*) <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-03-14/30893/> accessed 27 April 2020.

public authority or judicial orders, but constitute normal notifications under the ECD's NTD system. The CTIRU had identified and referred over 300,000 pieces of alleged terrorist content between 2010 and 2018, which were removed by the platforms concerned.[1045]

The tightening of online surveillance, stop and search, and access powers in the area of counter-terrorism online give more serious cause for concern over fundamental rights protections. Not only are the freedoms of respect for private and family life and protection of personal data of the targeted persons affected, but also those of their families, other contacts and indeed, anyone subject to state-ordered online surveillance.[1046] The more secretive and informal nature of cooperation between platforms and national authorities only adds to the existing opacity of content management decisions of these companies.[1047]

With the international and borderless nature of terrorism on the internet, police authorities, national intelligence and prosecution services need to exchange information and coordinate action increasingly fast. International cooperation therefore becomes crucial for the effective battle against terrorist acts on a national level. International cooperation on anti-terrorism measures was intensified after the 9/11 terror attacks in New York. Today, nineteen international agreements and instruments exist under the UN auspices to fight terrorism on an international level.[1048] However, the UN instruments have had only a limited impact on the international fight against terrorism on the internet. This is mainly due to the obstacles of cooperation between Western nations and other states, whose proposed restrictions are often perceived by the former as violating democratic principles.[1049] The Financial Action Task Force (FATF) is another international forum that is dedicated to the fight against terrorism. Initially set up to combat money laundering, its mandate was extended in 2001 to include the fight against terrorist financing.[1050] The 2001 Convention on Cyber-

1045 THERON Francois, 'Terrorist Content Online' (European Parliament 2020) Members' Research Service PE 649.326. 'Together We're Tackling Online Terrorism' (*Counter Terrorism Policing*, 19 December 2018) <https://www.counterterrorism.police.uk/together-were-tackling-online-terrorism/> accessed 23 September 2020.

1046 Castets-Renard (n 1039) 394.

1047 Citron (n 914) 26–27.

1048 Ballegooij and Bakowski (n 1018) 10.

1049 Walker and Conway (n 1041) 166.

1050 FATF, 'What We Do - Financial Action Task Force (FATF)' <https://www.fatf-gafi.org/about/whatwedo/> accessed 24 September 2020.

crime and its 2003 Additional Protocol are the first measures at European level aimed at establishing tools and cooperation processes in the fight against terrorist acts committed through computer systems.[1051]

The EU has a shared competency to regulate in matters that foster coordination and cooperation between Member States in the Area of Freedom, Justice and Security, thanks to its enlarged mandate following the 2009 Lisbon Treaty.[1052] It has a responsibility to ensure a high level of security as per Article 67 (3) TFEU. TFEU Articles 82 (1) (2) and 83 (1) allow it to propose legislation in the area of judicial cooperation and Article 87 with regards to police cooperation. Article 75 TFEU confers powers on the EU when it comes to combating the financing of terrorism. Where the fight against terrorism touches on the functioning of the internal market the EU can legislate based on Article 114 TFEU.[1053]

The EU has noted the potential of the internet for political radicalisation and the need to coordinate Member States' actions to prevent misuse of the web for terrorism since at least 2005, with the publication of its Counter Terrorism Strategy.[1054] It updated this strategy in 2015 with the Agenda on Security and made the fight against terrorism and cybercrime a priority.[1055] The EU has since brought in place a series of institutional arrangements and legal instruments aimed at supporting the fight against terrorism and cybercrime. The European Union Agency for Law Enforcement Cooperation (*Europol*) and the European Union Agency for Criminal Justice Cooperation (*Eurojust*) have been set up to support Member States in cross-border investigations, prosecutions, law enforcement and providing intelligence on serious crimes, including terrorism. Investigations and prosecutions of terrorist offences at EU level have been strengthened through joint investigations teams, European arrest warrants and the ex-

1051 Walker and Conway (n 1041) 12., Council of Europe - Convention on Cybercrime 2001; Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.

1052 Treaty on the Functioning of the European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2016) Article 4 (2) (j).

1053 Ballegooij and Bakowski (n 1018) Annex A, p. 112 - 114.

1054 European Council (n 1020) paras 9, 13.

1055 European Commission, 'The European Agenda on Security - COM(2015) 185 Final' (2015) ch 3.

change of criminal records. A number of information systems and databases facilitate cross-border access of data for law enforcement.[1056]

These cooperation measures are also aimed at keeping track of the increasing speed with which terrorist organisations act through the internet. The 2017 Directive on combatting terrorism obliges Member States to criminalise the distribution, regardless of whether on- or offline, of material that constitutes a public provocation to commit terrorist offences.[1057] Member States also need to ensure that terrorist content online is removed, or access to it blocked promptly, and subject to transparent procedures. This should happen with respect to the provisions of the ECD.[1058] *Europol's* Internet Referral Unit (IRU), established in 2015, supports the identification, flagging assessment and referral of terrorist content online for removal by online platforms. In addition, it supports Member States in monitoring and provides investigative capabilities regarding terrorist content online. Between July 2015 and 2018 it had identified close to 88,000 pieces of content and referred over 85,000 for action to online service providers, achieving a removal rate of 84.8%.[1059]

It should be noted that these efforts relate mainly to *ex-post* actions and law enforcement. The EU has also committed to developing counter-narratives and stepping up educational efforts such as developing inter-cultural dialogue and social inclusion in a bid to oppose the radicalisation of society.[1060] Meanwhile, the efforts to include social media platforms on any proactive technical measures to combat terrorist content on their systems are restricted to voluntary actions.[1061] At this stage, government actions towards social media platforms are limited to national level efforts that are often less transparent. It is not clear in how far hosting providers are informally involved in working with governments proactively to prevent terror-

1056 Ballegooij and Bakowski (n 1018) 16–17. Teresa Alegra Quintel, 'Interoperability and Law Enforcement Access to Personal Data. Data Protection Rights of Third Country Nationals in the Light of the CJEU's Case Law' [2018] Europarättslig tidskrift 7–8

1057 Directive (EU) 2017/541 on combating terrorism Article 5.

1058 ibid Article 21, Recital 6.

1059 European Union Agency for Law Enforcement Cooperation (n 1018) 76.

1060 European Commission, 'Radicalisation Awareness Network' (*Migration and Home Affairs - European Commission*, 6 December 2016) <https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en> accessed 28 April 2020.

1061 European Commission, 'The European Agenda on Security - COM(2015) 185 Final' (n 1054) ch 3.3.

ist content online. The EU contributes with capacity building and judicial and law enforcement cooperation to fight terrorist crimes on the internet.

III. Private regulation of terrorist content and technological developments

As in other areas, the EU has initiated self-regulatory projects with social media platforms to fight terrorist content online. Following on from the 2015 Agenda on Security the European Commission set up the EU Internet Forum, a self-regulatory structure, bringing together *Europol*, hosting providers and the European Parliament in a bid to establish "a joint, voluntary approach based on a public-private partnership to detect and address harmful material online."[1062] The initial membership from the industry, *Ask.fm, Facebook, Google, Microsoft* and *Twitter*, has now grown to over 20 hosting providers, and includes social media and UGC platforms, cloud providers, content management systems and messaging services. This private-public initiative has so far worked in different areas.

First, the industry members committed to participating in the EU's Civil Society Empowerment Programme that aims at developing counter narratives to terrorism on social media and UGC sites. This plugs into existing efforts of companies such as *Google, Facebook* and *Twitter* to post alternative messages and counter-adverts on pages that contain potentially extremist and terrorist content.[1063]

Secondly, the member companies are also the forum of choice for referrals by *Europol*'s IRU. Under this process, the participating platforms had removed 61% of referred content during the first half of 2018, with the "big four" (*Facebook, Microsoft, Twitter and YouTube*) removing between 90% and 100%. The majority of companies, however, did not manage to remove content within one hour of notification, an objective of the IRU in order to effectively prevent potential sharing and multiplication across the internet.[1064]

1062 European Commission, 'EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online' (*European Commission - European Commission*, 12 March 2015) <https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243> accessed 28 April 2020.

1063 Citron (n 914) 28–29.

1064 European Commission, 'Terrorist Content Regulation Proposal - Impact Assessment' (n 1024) 135.

Thirdly, the Forum also set up a shared industry hash database (SIHD) for terrorist content that allows its members to prevent the reappearance of content identified by one platform on other ones. In 2017, *Facebook, Google*, *Twitter* and *Microsoft* founded for this purpose the Global Internet Forum for Terrorist Content (GifTC). Through this initiative they pool resources and develop solutions to combat terrorist content online in cooperation with civil society and governments around the globe. As of 2019, the GifTC had another 5 members: *Amazon*, *DropBox*, *Pinterest, LinkedIn* and *WhatsApp*, while the Hash Sharing Consortium of the SIHD counted *Reddit*, *Snap*, *Verizon* and *Ask.fm* amongst its participants.[1065]

The hash database relies on technology that assigns a numerical value - hash codes or digital fingerprint - to images.[1066] Terrorist content identified by participants is hashed and may be enriched with metadata, such as the type of content, the terrorist group or the company that hashed and shared the content with the SIHD.[1067] According to GifTC, the SIHD contained over 200,000 hashes by 2019. Participants will be able to use the hashed content in order to identify and remove matching content that already exists or is uploaded to their systems where it breaches their policies. The particular technology used relies on perceptual hashing. The fingerprints are calculated based on certain characteristic features of the content. This method is more resistant to marginal modifications and allows for detection according to commonly identified characteristics or traits (of terrorist content), rather than exact matches. This technology is also closely related to mechanisms used in deep learning systems that aim to proactively detect content features.[1068] The exact processes and methods relating to the hash database and the way content is shared and used remain rather secretive, which is partly understandable given the highly sensitive techniques involved. Nor is it clear to what extent content hash-filtered during upload will be removed automatically or is subject to human review for a final decision.[1069]

1065 'GifCT' <http://www.gifct.org> accessed 28 April 2020.

1066 Brian A Jackson and others, *Practical Terrorism Prevention: Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence* (RAND 2019) 83.

1067 Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 205395171989794, 8.

1068 ibid 4.

1069 ibid 8.

Meanwhile, GifTC members have also increasingly engaged in the proactive, automated detection and blocking of terrorist content. As stated, the technology of perceptual hashing lends itself to the use in predictive content identification and classification. *Facebook*, for example, noted in its latest Community Standards Enforcement report that, for Q3 2019, 98% of terrorist content that it removed was detected by its own automated systems. Altogether, over 5.2 million pieces of content were removed, both by its own systems and through user notifications. Meanwhile, 205,300 pieces of content were restored again, of which 32,400 after an appeal.[1070] This makes for an overall decision accuracy rate of 96%.[1071] It is not exactly clear to what degree human reviewers at *Facebook* are involved in reviewing content decisions made by automated systems, but it appears that the exclusive use of these tools is increasing. Nevertheless, the company continues to beef up its army of content reviewers. The number of content reviewers employed or subcontracted by *Facebook* around the globe has risen to 15,000 by end November 2019.[1072]

Similar developments can be reported for *Twitter* and *YouTube (Google)*,[1073] and as a rule, for any larger online platform operator, which all use automated systems to detect and remove terrorist content, albeit to varying degrees. It should, however, not be forgotten that even with constantly improving detection tools, a content identification accuracy of 99% still means that the real number of falsely identified content is enormous.[1074] It can be safely assumed that it would be in the reputational and financial interest of any social media platform to contain the number of erroneous decisions by introducing human reviews.

1070 Facebook, 'Community Standards Enforcement Report - Terrorist Propaganda' (n 668).

1071 If one were to take the so-called reinstate rate as a measure for decision accuracy. Isabelle van der Vegt and others, 'Shedding Light on Terrorist and Extremist Content Removal' [2019] Royal United Services Institute for Defence and Security Studies 7.

1072 'Facebook's AI Wipes Terrorism-Related Posts' *BBC News* (29 November 2017) <https://www.bbc.com/news/technology-42158045> accessed 28 April 2020. Facebook, 'Understanding the Community Standards Enforcement Report' (November 2019) <https://transparency.facebook.com/community-standards-enforcement/guide> accessed 28 April 2020.

1073 Omi Hodwitz, 'Rule-of-Law and Respect for Human Rights Considerations' in John R Vacca (ed), *Online terrorist propaganda, recruitment and radicalization* (2020) 74. In addition see the regular transport reports on the enforcement of these companies' own community guidelines

1074 van der Vegt and others (n 1070) 8–9.

Smaller platforms, on the other hand, may not have the resources to develop and maintain automated software systems. Research and cooperation on automated removal systems has also been a focus area of the GifTC.[1075] It appears that the larger players share their respective technologies, such as *Microsoft's PhotoDNA* or *Google's Content Safety API*, which were developed originally to spot and remove child abuse material. These technologies may even assist smaller players.[1076] Nevertheless, human review of potential terrorist content still appears to be important. Larger platforms may use it in parallel to automated systems, while smaller players are more likely to rely on it exclusively.[1077] This does not necessarily disadvantage these latter companies, as content reviews can be scaled by other means than matching software. Behavioural patterns may, for example, also give useful clues about the propensity of content for being unlawful, e.g. terrorist.[1078] This can be supplemented by other risk management approaches.

Despite internet platforms rubbing elbows in self-regulatory circles like the GifTC, the criteria and processes by which terrorist content is defined vary across different platforms. For a start, the definition of terrorist content varies on a normative basis between the different companies.[1079] Globally operating platforms then also face varying and at times contradicting definitions and understandings of terrorist activity across jurisdictions. They often do not understand how to incorporate specific terrorist or sanctions lists issued by governments, civil society or academia, in their content policies.[1080]

Secondly, the internal enforcement procedures, ranging from content moderation procedures to the use of automated tools, appeals procedures through to the yardsticks for measuring efficacy and decision accuracy of identification and removal processes, vary. This may be due to several factors: different contextual situations of speech on platforms, varying business models of these platforms, different resource allocations or simply in-

1075 Gorwa, Binns and Katzenbach (n 1066) 9.
1076 Citron (n 914) 23; Gorwa, Binns and Katzenbach (n 1066) 8. Facebook mentions in its company blog that it utilises Microsoft and Google technology: Antigone Davis and Guy Rosen, 'Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer' (*About Facebook*, 1 August 2019) <https://about.fb.com/news/2019/08/open-source-photo-video-matching/> accessed 29 April 2020.
1077 van der Vegt and others (n 1070) 6–7.
1078 ibid 4–7.
1079 Citron (n 914) 22.
1080 Meserole and Byman (n 1028).

dividual company cultures, such as the fervency with which US-style free speech values are being pursued.[1081]

The next striking observation is that there is a considerable variance between platforms' enforcement systems of their own content standards and their policies with regards to notified terrorist propaganda. This extends to the referrals processes in place with *Europol* and national enforcement authorities. The low volume of referrals from IRUs (compared to platforms own enforcement actions), the relatively low removal rate and the closed nature of the GifTC's operations, point to the existence of parallel systems of terrorist content removals on these platforms.[1082] The IRU referrals processes stand in stark contrast to *Facebook* et al's sophisticated, scaled and fast enforcement of their own content policies. This reinforces arguments that these platforms, and not authorities, are acting as the *de facto* regulators in content regulation.[1083] Real states, meanwhile, face difficulties in getting these platforms to address the public interest concerns related to unlawful content.[1084]

Yet, concerns over the transparency and power of platforms' own content enforcement policies are as salient as concerns over a too intimate and closed relationship between law enforcement and platforms. In how far, however, social media intermediaries have really become global enforcers of stricter EU speech standards is less clear.[1085] Platforms appear more to enforce their own policies based on carefully concealed internal operational guidelines.[1086] They adapt to situations outside these terms and policies in a more haphazard and inconclusive manner. This points towards the dominance of economic reasons and cultural speech standards of their managers,[1087] to the detriment of compliance with local laws and public interests. In the end, Member States' IRU referrals are being decided against the private terms and conditions of these platforms and not against the legal norms that apply in the respective country. The exact power rela-

1081 Klonick (n 1000); van der Vegt and others (n 1070).
1082 van der Vegt and others (n 1070) 9
1083 Uta Kohl, *The Net and the Nation State - Multidisciplinary Perspectives on Internet Governance* (Cambridge University Press 2017) 12. Taddeo and Floridi (n 120) 1593; Belli and Sappa (n 42) 189–190.
1084 Ben Wagner, 'Governing Internet Expression: How Public and Private Regulation Shape Expression Governance' (2013) 10 Journal of Information Technology & Politics 389, 399.
1085 Citron (n 914) 29–30.
1086 Klonick (n 1000) 1635–1650.
1087 Zuboff (n 5) l 2012; Klonick (n 1000) 1644–1645.

tions between the state and platforms in these self-regulatory initiatives are far from clear and warrant further study.[1088]

All of this shows that the content removal processes of online platforms, in general, and in the case of hate speech and terrorist propaganda, in particular, are in dire need of more transparency. This concerns both the decisions taken by companies on their own account and those taken after referrals from authorities. But the current regulatory framework in the EU, does not provide for any mandate to prescribe more holistic content management obligations that comply with standards of transparency, accountability and corporate responsibility that are commensurate with the status of online platforms today.

IV. EU regulation

a. Proposal of a Regulation for preventing terrorist content online

In 2018, the European Commission introduced a proposal for a regulation aimed at preventing the dissemination of terrorist content online (TERREG).[1089] With this proposal, the Commission intends to tighten measures that it had urged Member States to take against the spread of terrorist propaganda in its Recommendation on tackling illegal content online, made only six months earlier.[1090] Although broadly addressing any type of unlawful content, that document contained specific recommendations on combating terrorist material.

The TERREG proposal's impact assessment notes that despite the self – regulatory efforts and progress made (e.g. through the EU Internet Forum), the security threat posed by terrorist content spread through hosting platforms remained considerable. It states as main problems the continued abuse of hosting service providers, particularly smaller ones, for these purposes and the inefficacy of preventing this content to spread and reappear across platforms.[1091] It identifies four problem drivers, which have also

1088 Gorwa (n 267) 13.

1089 European Commission, Proposal for a regulation on preventing terrorist content online, COM(2018) 640 final 2018.

1090 European Commission, 'C(2018) 1177 Final' (n 8).

1091 European Commission, 'Terrorist Content Regulation Proposal - Impact Assessment' (n 1024) 7–10. OECD, 'Current Approaches to Terrorist and Violent Extremist Content among the Global Top 50 Online Content-Sharing Services', vol 296 (2020) OECD Digital Economy Papers 296 6–7 <https://www.oe

been discussed above: 1) the legal fragmentation facing hosting providers under, *inter alia*, the ECD: this includes variations in NTD systems, procedural differences in removal orders, the parallel existence of informal removal procedures (e.g. the UK), different level of duties of care, national specificities in the imposition of transparency obligations regardless of the place of establishment of the ISSP.[1092] 2) Member States have difficulties in establishing effective relations with many, mostly smaller, platform operators.[1093] 3) and 4) relate to ineffective or uneven implementation of systems to detect and remove terrorist content, and their intransparency *vis-à-vis* users and public authorities. The Commission remarked that IRU referrals were not actioned fast enough, preventive efforts varied across platforms and automated systems lacked safeguards and transparency, which impacted user rights negatively.[1094]

The proposed TERREG has a number of important elements. First, it provides a broad overarching definition of terrorist content.[1095] Secondly, it obliges platforms to remove content notified under a court or authority removal order within one hour and act expeditiously on the assessment of referrals from authorities.[1096]

The proposal imposes for the first time the application of duties of care on hosting providers,[1097] suggests a procedural and transparency framework for the removal of content[1098] and specifies the use of proactive mea-

---

cd-ilibrary.org/science-and-technology/current-approaches-to-terrorist-and-violent-extremist-content-among-the-global-top-50-online-content-sharing-services_68058b95-en> accessed 19 March 2021. 'Analysis: ISIS Use of Smaller Platforms and the DWeb to Share Terrorist Content – April 2019 - Tech Against Terrorism' (29 April 2019) <https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/, accessed 19 March 2021.

1092 European Commission, 'Terrorist Content Regulation Proposal - Impact Assessment' (n 1024) 10–12.

1093 ibid 13–16.

1094 ibid 13–17.

1095 European Commission COM(2018) 640 final (n 1088) Article 2 (5).

1096 ibid Articles 4 & 5.For a detailed analysis of these parts of the proposal see: Gavin Robinson, 'The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online' [2018] eucrim - The European Criminal Law Associations' Forum <https://eucrim.eu/articles/commission-proposal-regulation-preventing-dissemination-terrorist-content-online/> accessed 6 April 2020.

1097 European Commission COM(2018) 640 final (n 1088) Article 3, Recital 12.

1098 ibid Articles 4, 8, 9, 10, 11.

sures by hosting providers, using a risk management approach.[1099] It was amended during the negotiation process with the European Parliament and the Council. The version discussed here was voted by the plenary in April 2019,[1100] before the European elections in September that year. Under the current version the hosting providers' duties of care specifies that they need to protect users from terrorist content in a diligent, proportionate and non-discriminatory way, and with due regard to fundamental rights.[1101] The European Parliament inserted language specifying that any such duties should not amount to a general obligation to monitor content. This can be seen as a reminder of the prohibition in Article 15 ECD.

Obligatory proactive measures under a proposed Article 6 have been turned into voluntary specific measures in the current European Parliament version. Again, the respect of the principles laid down in the ECD and the new AVMSD are being recalled. Any measures need to be proportionate and correspond to the risk and level of exposure to terrorist content and the fundamental rights involved. Member States have, however, the option of imposing specific measures on those hosting providers, which have received substantial numbers of removal orders. Substantial numbers are not defined in the proposal. The Commission's suggestion in Recital 19 to derogate from the sacrosanct Article 15 (1) of the ECD in exceptional circumstances was rejected by the Parliament. It would have allowed Member States to potentially impose obligations on hosting providers to monitor their systems on a general basis and proactively seek illegal information in situations of overriding public security concerns. The European Parliament held that this would result in a dramatic shift in intermediary liabilities and an excessive impact on fundamental rights.[1102]

The proposed reactive duties provide a procedural framework aimed at transparent and accountable content removal processes and reporting.[1103]

1099 ibid Article 6, Recital 16 & 19.

1100 European Parliament, 'Report on the Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online - A8-0193/2019' (2019) PE 632.087v02-00 <https://www.europarl.europa.eu/doceo/document/A-8-2019-0193_EN.html> accessed 30 April 2020. During the time of writing the Council and the European Parliament reached a political compromise on this proposal on 10 December 2020, which, however, maintains the key changes proposed by the European Parliament in the 2019 version analysed here. At the time of writing, the political compromise version was in the final stages of adoption.

1101 ibid Article 3.

1102 ibid Opinion of the Committee on Culture and Education (iii).

1103 European Commission COM(2018) 640 final (n 1088) Articles 8, 9, 10, 11.

Article 9 asks providers that use automated tools to have safeguards in place that ensure the appropriateness of content decisions, especially with regards to fundamental rights. Such safeguards would be, for example, verification procedures and human oversight. The European Parliament version of April 2019 enhances user rights by imposing more detailed remedies in cases of content removals, such as explanations from the platform about the removal and more detailed appeals procedures.[1104] However, the obligation to publish annual transparency reports has been limited to only those platforms that were subject to removal orders for authorities or courts. The providers concerned would need to publish annual accounts on the detection, identification and removal of content. They also have to detail their efforts to prevent the re-upload of content, especially where automated means are used, state the numbers of content removals following an order, and the numbers and outcomes of complaints following a removal.[1105]

The TERREG proposal is probably the most far reaching effort by the EU legislator so far to regulate the framework conditions for online intermediaries in the prevention of unlawful content. It may be no surprise to see the proposed emergency cancellation of the general monitoring prohibition of Article 15 (1) ECD being rolled back by the European Parliament. However, the original attempt of the Commission may be a demonstration of the interpretational problems this 20-year-old provisions causes in today's social media platforms environment. The obligatory use of automated tools to prevent terrorist content has been toned down to a voluntary encouragement of specific measures. However, the option to impose specific (read: proactive) measures has been kept for those riskier platforms that have received removal orders from Member States' courts or authorities and where the latter determine that the current measures are not sufficient. The transparency obligations for those platforms that deploy specific measures and that are subject to removal orders may go a certain way towards more accountability and openness. However, the proposal lacks a more solid institutional substructure at an EU level that would accompany, supervise and drive the implementation of consistent accountability and risk management structures. Although it requires Member States to nominate a functionally independent authority for issuing removal orders, overseeing specific measures of hosting providers and imposing penalties, the level of cooperation between them in order to build consistent struc-

1104 European Parliament (n 1099) Articles 10, 11.
1105 ibid Article 8.

tures and processes is not further specified.[1106] By contrast, the AVMSD which also foresees the application of proactive measures following a risk-based approach, puts in place an EU wide regulatory body (ERGA) to accompany and supervise this process. This may be more effective in the medium term. As it stands now, the partly far-reaching specific measures and transparency obligation on platforms in the proposed regulation risk fizzling out without an EU wide institutional framework that forces coherent and unified reporting and accountability standards.

b. Regulation 2019/1148 on marketing and use of explosives precursors[1107]

In 2019, the EU enacted a new regulation that imposes due diligence operation on online marketplaces in the fight against the unlicensed sale of chemicals that can be used to fabricate explosives for terrorist attacks.[1108] This Regulation does not cover digital content related to terrorism as covered above. However, it shall be included here, and not in a later section on unsafe products, because of the potential use of these substances for terrorist acts. The Regulation falls therefore into the wider context of the misuse of the internet and online intermediaries for terrorism-related crimes and the hams to public security covered in this section.

According to the European Commission "explosives precursors are chemical substances habitually used for legitimate purposes, but that can also be misused to manufacture homemade explosives."[1109] Explosives precursors can be, just to give two examples, sulphuric acid, which is widely used in industry but also in agriculture; or ammonium nitrate, which is

---

1106 ibid Articles 9 (a), 12, 13, Recital 37.

1107 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors 2019 (OJ L 186).

1108 See also: Anja Hoffmann and Alessandro Gasparotti, 'Liability for Illegal Content Online - Weaknesses of the EU Legal Framework and Possible Plans of the EU Commission to Address Them in a "Digital Services Act"' (cep | Centre for European Policy 2020) 21 .

1109 European Commission, 'Counter Terrorism and Radicalisation - Protection' (*Migration and Home Affairs - European Commission*, 6 December 2016) <https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en> accessed 26 August 2020.

used as a fertiliser.[1110] In the Impact Assessment for this Regulation, the European Commission notes that, amongst other problems with the enforcement of registration and verification duties regarding the sale of these substances, explosive precursors have continued to be available for purchase by terrorists in the EU partly due to a shift towards e-commerce, where restrictions were applied less diligently.[1111] It states that precursors used in the fabrication of explosives that were deployed in recent terrorist attacks in the EU had been purchased online. The anonymity and the difficulty of tracing customers in transactions conducted via online marketplaces, the problems in detecting the products in question and identifying suspicious transactions pose a new security threat.[1112]

While adding new substances to the restricted substances list and tightening overall registration, licensing, verification, detection and reporting obligations of economic operators, the Regulation now also includes online marketplaces in its scope. It acknowledges the central role of online marketplaces in online transactions and the availability of regulated explosive precursors, but stops short of qualifying online marketplaces as economic operators.[1113] The obligations imposed on online marketplaces are therefore lighter than for economic operators. The former are not required to pass on information on the acquisition and possession of restricted precursors along the supply chain or assure that their staff are adequately trained.[1114] They also do not need to apply customer verification processes, such as identity checks or requesting evidence of the intended use of the substances sold.[1115]

However, online marketplaces would need to ensure that users (in this case sellers) that offer regulated explosives precursors on their platforms are aware of their obligations and support them in their compliance with verification duties.[1116] Online marketplace will have, nevertheless, the same obligations as economic operators when it comes to detecting and re-

1110 European Commission, 'Commission Staff Working Document - Impact Assessment - Proposal for a Regulation of the European Parliament and of the Council on the Marketing and Use of Explosives Precursors - SWD(2018) 104 Final' (European Commission 2018) 93–94.
1111 ibid 10–12.
1112 ibid 91.
1113 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors Recital 15.
1114 ibid Article 7.
1115 ibid Article 8.
1116 ibid Articles 7 (3) & 8 (5).

porting suspicious transactions.[1117] These detection measures shall be appropriate, reasonable and proportionate and adapted to the specific environment. Recital 16 of the Regulation clarifies that the obligations imposed on online marketplace shall not lead to a general monitoring obligation, but remain specific to the detection and reporting of suspicious transactions. Online marketplaces that have reasonable detection procedures in place shall not be liable for any transactions that they fail to pick up. When it comes to reporting suspicious transactions, the regulation provides five (non-exhaustive) indicators that would trigger a notification to the authorities. Two of these indicators appear to be relevant for online marketplaces: reporting may be triggered when customers buy quantities or combinations of products that are uncommon for legitimate use, and where customers use unusual payment methods, such as cash.[1118]

The detection and reporting obligations take account of the fact that most online marketplaces today widely collect and utilise data on consumer purchases, browsing behaviour, seller sales and marketing analytics. They are indeed in a central position, not just when it comes to facilitating the availability and marketing of products, but also where market intelligence about the supply and demand of products is concerned. The reporting obligations remind of existing obligations in the area of anti-money laundering, where financial institutions, including electronic payment services or electronic money institutions, have already suspicious transaction monitoring and reporting obligations. Most online marketplaces integrate payment services into their platforms. Where they do not offer their own payment service, like *AmazonPay* or *AliPay*, they integrate other service providers such as *PayPal*, *GooglePay*, major credit cards or other providers into their platforms. Some elements of transaction monitoring under these obligations, or under existing internal fraud detection processes, should therefore be familiar to most online marketplaces. Subsidiaries of *Amazon*, *Rakuten*, *eBay* or *AliExpress* are all registered as banks, payment institutions or electronic money institutions in the EU.[1119]

1117 ibid Article 9.

1118 ibid Article 9 (1). Note that some online marketplace like *eBay* or *CDiscount.com* offer cash and/or cash on delivery as payment methods: 'Artikel Bezahlen' (*eBay*) <https://www.eBay.de/help/buying/paying-items/artikel-bezahlen?id=4009> accessed 26 August 2020; 'Cdiscount.com Payment' (*CDiscount*) <https://www.cdiscount.com/payment/paymentinfo.html> accessed 26 August 2020.

1119 For further detail see the section on trademarks in this Chapter.

Meanwhile, the requirement to ensure that sellers are aware of their obligations under the Regulation and to help them in their efforts to put in place customer verification measures, takes advantage of the gatekeeping functions of today's online marketplaces. First, marketplaces are able to put detailed information and qualification processes in place when they onboard sellers on their platforms. This can very well include specific education and information processes. These processes can be narrowed down to product categories and certain seller characteristics. This will be shown in more detail in the section on consumer protection, the case studies in Chapter 5 and the example of a duty of care standard for economic harms provided in Chapter 6 and ANNEX III. Secondly, online marketplace can indeed provide additional leverage when it comes to customer verification. They provide the technical facilities for marketing, sale, transactions and customer communication. In order to buy through an online marketplace, customers would normally need to be registered or create an account on the marketplace. Online marketplaces are able to insert additional customer verification processes into the transaction chain, or offer sellers the option for integrating these steps into their own transactions. Finally, online marketplaces also have the ability to check and audit compliance with these procedures.

Smaller marketplaces may indeed not be well equipped to comply with all of these obligations to the same extend as larger operators. But it can be argued that, as diligent economic operators, smaller marketplaces that choose to include more highly regulated, risky product categories on their platform would still have to be aware of the potential harm that could be caused by selling these products. This also exposes the gap in the current online intermediary liability framework of the ECD. An almost blanket exemption absent any 'actual knowledge' fits uncomfortably with the wide reach of activities of today's online marketplaces and other online intermediaries.

The regulation also appears to provide a procedural framework for enforcement and supervision. It tasks Member States with facilitating cooperation and exchange of information between law enforcement, national supervisory authorities, economic operators, online marketplaces and representatives of the sectors that use regulated explosives precursors. The European Commission will need to provide guidance on measures that online

marketplaces may adopt under the Regulation. Meanwhile national authorities will need to inspect and control effective compliance.[1120]

Overall, the regulation goes a significant way in imposing enhanced responsibilities on online marketplaces that appear to fit into a wider due diligence or duty of care framework. These obligations appear adequate and commensurate with the gatekeeping function of today's online marketplaces. On the other hand, it stops short of qualifying online marketplaces as economic operators. Arguably, this is a missed opportunity. The crucial position of online marketplaces when it comes to seller and customer onboarding and transaction monitoring extends into other aspects, such as online product information (e.g. online labelling and warning requirements). Here too, they may affect essential requirements relating to the product itself. Secondly, by making money from the sale of these products, either through a commission on sales, seller fees or advertisements related to the online offer, online marketplace clearly have a financial interest in the transactions of explosive precursors. In the area of copyright and trademarks this has been a determining element for courts in allocating primary liability to online intermediaries. The procedural framework for effective implementation and compliance, however, is closer to traditional state regulation. Whether it provides space for defining more detailed due diligence criteria through active participation of economic operators and marketplace operators remains to be seen. A co-regulatory approach may be possible though the commitment to a wider stakeholder dialogue in Article 10 (3). Opening these circles to civil society and/or regular reporting would certainly be a safeguard against the risk of scope creep in the detection and reporting obligations imposed on online marketplaces and economic operators.

Like in the area of hate speech, new horizontal due diligence obligations under the DSA proposal would apply without prejudice to the proposed TERREG and to Regulation 2019/1148 on explosives precursors,[1121] thus confirming the *lex specialis* status of the latter. Potential overlaps or conflicts could arise between orders to act against illegal content under the current DSA proposal[1122] and removal orders by law enforcement authorities for terrorist content under the proposed Regulation on terrorist content online. While under the DSA proposal these illegal content removal

1120 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors Articles 1- - 12.
1121 European Commission DSA proposal (n 10) Article 1 (5), Recitals 9, 10.
1122 ibid Article 8, Recital 30.

orders are part of the liability exemption conditions, failure to implement removal orders under the Regulation are subject to penalties.[1123] Secondly, the implementation of the traceability obligations that online marketplace will have *vis-à-vis* traders on their platforms under the proposed DSA[1124] could significantly help in the execution of the information, detection and reporting requirements on the sale of explosive precursors under Regulation 2019/1148.

V. Summary and outlook

In December 2020, the European Council announced a provisional agreement with the European Parliament in the negotiation of the TERREG.[1125] The compromise appears to retain the key provisions set out in the version analysed above. It confirms the notion of duties of care and specific measures that hosting service providers exposed to terrorist content would need to take under a risk-based approach, although in a toned down version. It bolsters, however, the overall safeguards to protect fundamental rights when platforms use specific and automated tools to detect and remove terrorist content. Notably, it specifies that hosting providers should be under no obligation to use such automated tools.[1126] It also keeps the scope of the transparency obligations. Nevertheless, this latest compromise refrains from defining more tangible specific measures and from creating stronger institutional and procedural structures at EU level. The proposed Regulation goes in the right direction in proposing additional responsibilities for social media platforms in the fight against terrorist content. It re-

1123 European Commission, European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)) Article 18 (1).

1124 European Commission DSA proposal (n 10) Article 22.

1125 Council of the EU, 'Terrorist Content Online: Council Presidency and European Parliament Reach Provisional Agreement' (10 December 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/12/10/terrorist-content-online-council-presidency-and-european-parliament-reach-provisional-agreement/> accessed 15 March 2021.

1126 Council of the EU, 'Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online - Analysis of the Final Compromise Text with a View to Agreement 2018/0331(COD) - 12906/20' <https://data.consilium.europa.eu/doc/document/ST-12906-2020-INIT/en/pdf> accessed 15 March 2021 Article X, Recital 16, 19.

mains unclear, however, how these proposed platform responsibilities would be supervised, checked and enforced. It remains to be seen how the additional due diligence obligations of the DSA proposal will interact with this draft Regulation.

Regulation 2019/1148 on marketing and use of explosives precursors imposes relatively broad verification, detection and reporting obligations on online marketplaces for the sale of explosive precursors. These measures are a direct response to a shift of the availability of these products through online marketplaces and the increased risk of this channel being used by terrorists to procure components for explosives. They take account of the central gatekeeping role of online platforms in e-commerce by imposing specific detection and reporting obligations and asking platforms to assist sellers in their compliance efforts. The measures remind of existing duties under EU anti-money laundering legislation. This raised standard of responsibility is accompanied by a procedural framework under the auspices of the European Commission and national authorities. While encouraging stakeholder cooperation and exchange of information, the measures would gain in transparency if the circle was opened to wide society participation and regular reporting obligations. Overall, the obligations imposed on marketplace operators would be bolstered through the due diligence obligations on the traceability of traders that are proposed in Article 22 of the DSA draft.

Self-regulatory efforts, by contrast, have gone only a limited away to appease public security concerns in this respect. Platforms have developed and shared technical know-how in the fight against the terrorist threat online that appears to bypass enforcement authorities. The mass of their referrals is filed against the private content policies of these platforms rather than legal provisions. This current practice entrenches the position of these platforms as quasi regulators of speech that follow privately set standards and rules, be it in the area of defamation, hate speech or terrorist content. It should be noted, however, that the interactive and participative role of social media platforms is less controversially discussed in the area of terrorist content online than for violations in the areas of defamation and hate speech. Rather than challenging the role of platforms as potential editors of terrorist content, national law makers have defined specific crimes that relate to dissemination of this material via electronic media. While this rules out the allocation of primary responsibilities to platforms as terrorist speech editors, it does pose the question what dissemination actually means in the age of social media and content sharing. This touches directly

on the roles and responsibilities of social media platforms for hosted and shared content, which is the centrepiece of their business model.

It is submitted here that without widening and consolidating the general responsibilities of these platforms under current EU intermediary liability rules, the efforts of the proposed Regulation will remain piecemeal and do little to effectively address public security concerns. A redraft of these intermediary liability exemption or responsibility provisions would have the advantage of redefining the wider moral and normative responsibilities of social media platforms. This would then provide a basis for defining procedural obligations in the area of terrorist content online and supplement them with an institutional regulatory framework to supervise and enforce these obligations.

C. Economic rights: intellectual property

4. Copyright

I. Copyright and the information society

Copyright disputes have affected internet intermediaries since the early days of the commercial web. This is not surprising. Conflicts in copyright are imputed by the very nature of the internet, in which information is not sent in the traditional way, but where every transmission is an act of copying. The sender will not lose the information sent, as much as the addressee will not be its sole proprietor. Meanwhile, numerous copies, both transient and permanent, are being made at network interconnections and servers that lie along the globally dispersed communication channels.[1127]

Social networking, UGC sites or P2P systems facilitate the sharing (read: copying) of content at an unprecedented speed and to an audience with global reach that cuts across (almost) any jurisdiction. This is bound to conflict with the territorial and proprietary characteristics of copyright.[1128] Users, far from just consuming copyright protected works, are now engag-

1127 James J Marcellino and Melise Blakeslee, 'Fair Use in the Context of a Global Computer Network–Is a Copyright Grab Really Going On?' (1997) 6 Information & Communications Technology Law 137.

1128 H Bosher and S Yeşiloğlu, 'An Analysis of the Fundamental Tensions between Copyright and Social Media: The Legal Implications of Sharing Images on Instagram' (2019) 33 International Review of Law, Computers & Technology 164, 165.

ing in copyright relevant acts by uploading, sharing, modifying or reusing content at a massive scale. These acts have become commonplace and normal. People upload personal content enhanced by their favourite music tracks on *Facebook.* Musicians sample, create and share covers or remixes of songs on *YouTube* or *SoundCloud.* Users modify or replicate images of personalities, buildings or objects on social messaging apps, such *Instagram*, *TikTok* or *Snapchat* or web blogs.

For the Web 2.0 platforms, this user interaction is of course the mainstay of their business. It generates valuable user data and the advertising revenue that they have been thriving on. The undisputed benefit of the new exchange and creation of content for cultural and socio-economic enrichment has, however, been accompanied by more detrimental behaviours. Illegal downloading, P2P file sharing, streaming, or unauthorised sharing or reusing of content are the more common behaviours that remain widespread as of today.[1129] Some of these activities happen simply out of user ignorance over the intricacies of copyright law, or, like piracy, may also be due to a lack of legal offers on the market.[1130] Others are linked to organised crime.[1131] Some users and operators also challenge the entire concept of copyright or advocate for a significant reduction in its scope of protection.[1132] Some followers of these ideas, like the operators of *The Pirate Bay* P2P file sharing system, would intentionally disregard copyright regulations.[1133]

Online intermediaries have been in the main line of fire over their role in facilitating what rightsholders perceive as massive unauthorised distribution and communication of protected works. Music labels, film producers, copyright collecting societies and authors have lamented over substan-

---

1129 Tatiana-Eleni Synodinou, 'Copyright Law: An Ancient History, a Contemporary Challenge' in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) 98.

1130 Red Points, *Millennials and Piracy - Behaviour, Trends and Future Planning* (2016) <https://meet.redpoints.com/lp-203-ebook-millennials-and-piracy/> accessed 7 May 2020. João Pedro Quintais and Joost Poort, 'The Decline of Online Piracy: How Markets – Not Enforcement – Drive down Copyright Infringement' (2019) 34 American University International Law Review 807.

1131 EUIPO and Europol, 'Intellectual Property Crime Threat Assessment' (2019) 27–29.

1132 Michele Boldrin and David K Levine, *Against Intellectual Monopoly* (Cambridge Univ Press 2010). Shelly Warwick, 'Is Copyright Ethical? An Examination of the Theories, Laws and Practices Regarding the Private Ownership of Intellectual Work in the United States' [1999] B.C. Intell. Prop. & Tech. F.

1133 *Stichting Brein II* (n 214) para 45.

tial revenue losses and the erosion of their business models over the last 15 years.[1134] They have pursued not only the originators of unauthorised sharing and exploitation of works but also online intermediaries, internet access or hosting providers, in order to enlist them in their cause to prevent and remove infringing content.[1135] This battle has been going on despite of disagreement over the real economic damage caused by copyright violations and valid arguments over traditional publishers' failure to adapt to the internet age.[1136]

Some of the first cases in intermediary liability have dealt with these substantive challenges that rightsowners owners have faced when their works were shared and copied though bulletin boards or file sharing services without authorisation.[1137] Since then, copyright has probably become the most prominently analysed and debated content area in the context of intermediary liability, both from a policy and from an academic perspective.[1138]

This is due to several reasons. First, copyright, as an intellectual property right rests on a careful balance between potentially conflicting interests: while the property rights of the author are protected as a fundamental right,[1139] they are not absolute. They may be restricted by other fundamental rights and legitimate interest, such as the right to freedom of expres-

1134 For data see for example: Frontier Economics, 'The Economic Impacts of Counterfeiting and Piracy - Report Prepared for BASCAP and INTA' 38. This reports estimates the value of digital piracy film, music and software at $213 billion in 2015.

1135 Kristofer Erickson and Martin Kretschmer, 'Analyzing Copyright Takedown of User-Generated Content on YouTube' [2018] JIPITEC 75, 78–79; Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 281–285.

1136 Quintais, 'Global Online Piracy Study' (n 30) 23–27.

1137 See Chapter 3 see for example the cases of *Playboy Enterprises, Inc v Frena* (1993) 839 F. Supp. 1552 (MD Fla); *Sega Enterprises Ltd v MAPHIA* (1994) 857 F. Supp. 679 (Dist Court, ND Cal); *CDBench, 6 U 5475/99* [2000] MMR 2000 617 (OLG München). *Madame L. v. les sociétés Multimania Production, France Cybermedia, SPPI, Esterel* (n 362). It should be mentioned that the weight accorded to different rights varies between the US (Anglo-Amercian) and the European Continental traditions, especially were moral rights and copyright exemptions are concerned. MacQueen and others (n 345) 44–45.

1138 Carsten Ullrich, 'Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective' (2017) 8 JIPITEC 111, 114.

1139 CFREU Article 17 (2).

sion, the right to privacy,[1140] cultural interest and the freedom to conduct a business.[1141]

After bulletin boards and file sharing applications, the upcoming Web 2.0 intermediaries accelerated the use of new creative and communicative practices. Collaborative creation, mashups, linking and sharing would all be less popular and prevalent had it not been for the likes of *YouTube*, *Facebook, DailyMotion*, *Instagram or Google Search*, and thousands of other information hosts, including filesharing services. Online intermediaries have spurred the mass consumption of content and the mass participation of users in new content creation and sharing, providing ground-breaking new means for expression and cultural value. This has shaken the balance that copyright has sought to establish. The complex and intricate protections of copyright and their exceptions and limitations, became suddenly relevant for large swathes of the population in their daily use, as they interact via online platforms. This has led to consumer confusion and insecurity.[1142]

Secondly, intermediaries as hosts of third-party content and gatekeepers to the internet portray themselves as mere middlemen in order to minimise liabilities for the content they host. In reality, however, not only have they massively profited from their central position. Their content management decisions influence and steer user behaviour towards more interaction and tenure on the platform, inciting more communication and content creation. As explained already, this is done first and foremost for commercial reasons to create traffic, data, advertising and sales. The controversial question is whether these more intrusive platform business models interfere more directly in the substance of copyright.

Thirdly, copyright is primarily an economic right. As mass entertainment and media have spread increasingly through the internet and digital communications, online platforms have eaten into the cake comfortably enjoyed by established media and entertainment companies for decades. Despite being relative newcomers, *Google* and *Facebook* alone have been upsetting worldwide media advertising markets within less than a decade, diverting ad spend revenue away from TV and print media. While, for example in the US, traditional media (TV, print and radio) attracted 81% of advertising spending in 2010, their share had fallen to 49% within a span

1140 *Promusicae* (n 140).
1141 MacQueen and others (n 345) 243–244. *SABAM v NetlogSbtekel* (n 460) para 51; *Scarlet Extended* (n 139) para 53.
1142 Bosher and Yeşiloğlu (n 1127) 166–179.

of only eight years.[1143] Established media rightsowners have repeatedly claimed that this shift happened on the back of unlicensed or unlawful content shared freely by internet platform users. The ensuing economic battle has played out in major litigations, lobbying campaigns and policy initiatives worldwide. Copyright has therefore influenced significantly overall intermediary liability approaches as well as the way how online platforms today regulate content, both from a legal as well as a technological perspective.[1144]

The evolving adjustments of substantive copyright law to the internet era will not be fully recounted here.[1145] This section will focus on copyright where it touches on the role and responsibilities of online intermediaries, by paying attention to IAPs and hosting providers.

II. International law and EU set-up

Copyright law is partly harmonised through EU legislation. The starting point for this has to be sought at a global level. The 1996 WIPO Internet Treaties[1146] adapted copyright law to the digital age by supplementing the Berne and Rome Conventions that protect the authors of literary and artistic works and the rights of performers and producers, respectively.[1147] Most importantly, the WIPO Internet Treaties grant authors the public communication and distribution rights. The WIPO Copyright Treaty Article 11 also authorises the application of technical protection measures to copyright works. The provisions of the WIPO Treaties were transposed into EU law by the Infosoc Directive in 2001. This Directive is the first instrument that introduced a horizonal harmonisation of core aspects of copyright law.[1148] The EU competency to act in his area rests on today's Article 114 TFEU, which allows the EU to approximate national laws where this serves the establishment and functioning of the internal mar-

1143 Meeker (n 138) 22.
1144 Cornils (n 481) 17; Helman and Parchomovsky (n 309) 1195.
1145 For in-depth analyses see: Jütte (n 30); Schmitz (n 30); Synodinou, 'Copyright Law: An Ancient History, a Contemporary Challenge' (n 1128).
1146 WIPO Copyright Treaty (WCT) 1996 Articles 6 - 8 ; WIPO Performances and Phonograms Treaty (WPPT) 1996 Articles 6 - 8.
1147 Berne Convention for the Protection of Literary and Artistic Works 1886; Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations 1961.
1148 Jütte (n 30) 111–113.

ket.[1149] This underlines the economic dimension and motivations behind copyright.[1150]

On the one hand, the Infosoc Directive harmonises the core economic aspects of copyright through the rights of distribution and reproduction and the communication and making available to the public.[1151] National legal disputes and ambiguities of these rights and their application to the internet have been consistently harmonised at EU level, either through CJEU intervention or though EU policy action, especially where it concerns the rights of communication to the public and making available.[1152] Internet intermediaries enter into the frame of this discussion through the practices of hyperlinking and direct content hosting and sharing.

On the other hand, Member States are left with a margin of implementation when it comes to exceptions and limitations of copyright as per Article 5 of the Infosoc Directive. The exceptions provide for flexibility where copyright would conflict with other legitimate uses that are in the public interest or protect fundamental rights. The exceptions and limitations to the reproduction and communications rights in Article 5 Infosoc Directive are of special relevance to the internet and its intermediaries. It provides an exhaustive list of optional exceptions and limitations and one mandatory exception. For example, Member States are allowed to exempt the distribution of copies and the communications to the public from authorisation where this: happens for research and teaching purposes; concerns current economic or political news reporting, political speeches, and is part of quotations or criticisms, parody or caricature. Although the CJEU has stipulated that the exceptions, where implemented by national law, have an autonomous (unified) meaning under EU law,[1153] their voluntary character has resulted in a *de facto* fragmentation of copyright law.[1154]

1149 Directive 2001/29 (InfoSoc Directive) Recitals 1 - 3.

1150 Savin (n 384) 176.

1151 Directive 2001/29 (InfoSoc Directive) Articles 2 - 4.

1152 Tatiana-Eleni Synodinou, 'Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society' in Arno R Lodder and Andrew D Murray (eds), *EU regulation of e-commerce: a commentary* (Edward Elgar Publishing 2017) 66–75.

1153 Laid down for the parody exception by the CJEU in *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others, C-201/13* [2014] EU:C:2014:2132 (CJEU). As mentioned by: Synodinou, 'Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society' (n 1151) 80.

1154 P Bernt Hugenholtz, 'Why the Copyright Directive Is Unimportant and Possibly Invalid Hugenholtz' (2000) 22 European Intellectual Property Review 499,

The exceptions play a key role in protecting user rights but also in giving certainty to authors and rightsholders.[1155] Not making them equally applicable in all Member States has therefore been seen as signalling a certain carelessness for the public interest aspects of copyright compared to the economic preoccupations of rightsowners.[1156] The exhaustive list of exceptions makes for a certain inflexibility with regards to new uses of works engendered by e.g. UGC platforms. It has been notoriously difficult for online platforms and for users to understand exceptions like parodies, review or criticism, or political use as they apply to new forms of UGC, such as mashups, remixes and parodies. This is made even more complex when these exceptions do not apply consistently across all Member States.[1157]

The role of intermediaries in copyright law is addressed by Article 8(3) of the Infosoc Directive. This offers rightsholders the option to apply for injunctions against intermediaries that are used by a third party to infringe copyright or related rights. IPRED complements this by providing for the availability of injunctions against intermediaries in Articles 9 (1) and 11, as per the Infosoc Directive. However, IPRED and the Infosoc Directive both apply without prejudice to the liability provisions formulated under the ECD.[1158] The ECD therefore ties in with IP legislation and can be seen as supplementary to copyright law, similar to the provisions of data protection law.[1159] Any injunctions against intermediaries have to be in respect of the principles laid down in the ECD, specifically those that prohibit the imposition of general monitoring obligations. Meanwhile, the procedural and administrational detail of the injunctions and sanctions that intermediaries can be subjected to are regulated by national law.

501; Lucie Guibault, 'Why Cherry-Picking Never Leads to Harmonisation: The Case of the Limitations on Copyright under Directive 2001/29/EC' (2010) 1 JIPITEC 55.

1155 Christophe Geiger and Francisca Schönherr, 'Limitations to Copyright in the Digital Age' in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) 114.

1156 Savin (n 384) 193.

1157 Jütte (n 12); Erickson and Kretschmer (n 1134).

1158 Directive 2004/48 (IPRED) Article 2 (3); Directive 2001/29 (InfoSoc Directive) Recital 16.

1159 Synodinou, 'Copyright Law: An Ancient History, a Contemporary Challenge' (n 1128) 97–98.

III. Copyright enforcement and online intermediaries

a. Enforcement at Member State level

Member States have used the liability provisions of the ECD in conjunction with the intermediary enforcement options available under the Infosoc Directive and IPRED in order to enlist intermediaries in the fight against copyright infringements. But the Infosoc Directive and IPRED leave the conditions and modalities of such injunctions to Member States' national laws.[1160]

Therefore, the application of the ECD in the area of copyright is characterised by the generally diverging legal attitudes towards intermediary liability and the various remedies available through national laws. The disparate nature of the application of the liability provisions and the enforcement *vis-à-vis* intermediaries in copyright infringement cases has been analysed in great detail.[1161] Ample case law has been building up over the last 20 years to support this research. Intermediary liability in copyright can be seen as a showcase example for the fragmented and ambiguous landscape of enforcement against IAPs and hosting providers in Europe.[1162] A large part of the cases used to demonstrate the enforcement challenges of the ECD in Chapter 3 deal with unlawful acts in the area of copyright. This section will provide an overview by drawing on the rich literature on the subject.

As in other sectoral areas, some Member States, like for example the UK (when it was still in the EU), chose to look at intermediary liability conditions through specific provisions in their copyright or other statutes. Meanwhile, others, such as Germany, apply their civil law doctrine of *Störerhaftung* directly to intermediaries in copyright infringement cases.

1160 Directive 2001/29 (InfoSoc Directive) Recital 59; Directive 2004/48 (IPRED) Recital 23. Martin Husovec, 'Injunctions against Innocent Third Parties': (2013) 4 JIPITEC 14. Eleonora Rosati, 'Intermediary IP Injunctions in the EU and UK Experiences: When Less (Harmonization) Is More?' (2017) 12 Journal of Intellectual Property Law & Practice 338, 22.

1161 See for example in the following works: Angelopoulos (n 30); Schmitz (n 30); NaNM van Eijk and others, 'Moving Towards Balance: A Study into Duties of Care on the Internet' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1788466 <https://papers.ssrn.com/abstract=1788466> accessed 13 May 2020. Graeme B Dinwoodie, 'A Comparative Analysis of the Secondary Liability of Online Providers' in Graeme B. Dinwoodie (ed), *Secondary liability of internet service providers* (Springer Berlin Heidelberg 2017).

1162 Angelopoulos (n 30) 177.

In the UK, judges have tried to approach intermediary liability in copyright through the legal instrument of authorisation under section 16 of the Copyright, Designs and Patents Act (CDPA)[1163] or, alternatively, the common low doctrine of joint tortfeasance. By contrast, English courts have rarely made use of the tort of negligence, which would eventually lead to defining reasonable duties of care.[1164] This would be in line with the relative unease of common law jurisprudence with broader principles for positive obligations.[1165] The possibility of injunction against intermediaries involved in copyright infringements, provided for by Article 8(3) IPRED, was established by section 97A of the CDPA in 2003. It gives courts the power to grant an injunction against an ISSP, where the latter has actual knowledge of being used by someone else to infringe copyright. Actual knowledge is established through a notice which must contain the name and address of the sender and details of the infringement.[1166]

In France, the actions of intermediaries in copyright infringements are regulated through the aforementioned Article 6 of the LCEN. Injunctions against intermediaries are possible through the *Code de la Proprieté Intellectuelle (CDI)*Article L336-2 which was amended in 2006 in response to the Infosoc Directive.[1167] In parallel to these provisions, French courts make use of the *Code Civil's Articles 1240 and 1241* that deal with third party liabilities[1168]

Germany regulates the civil liabilities of infringers in Art 97 of the Law on Copyright and Related rights.[1169] As regards intermediaries that are found to qualify for the exemptions of the ECD, the German law applies its interferer liability doctrine, which relies on negligence-based considerations but will only result in the imposition of injunctions, and not dam-

1163 Copyright, Designs and Patents Act 1988 c.48.
1164 Angelopoulos (n 30) 94–120.
1165 See Chapter 3
1166 Copyright, Designs and Patents Act 1988 c.48 s 97 A.
1167 LOI n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information. See also the explanation in the judgement *SNEP v Microsoft France et Microsoft Inc* (2016) (Unreported) (Tribunal de grande instance de Paris).with respect to search engine Bing
1168 *Jean-Yves Lafesse et autres v Google et autres* (n 553); *Roland Magdane et autres v Dailymotion* (n 607). where the relevant Articles of the *Code Civil* were still 1381 and 1382
1169 Gesetz über Urheberrecht und verwandte Schutzrechte Article 97.

ages.[1170] Since 2008, intermediaries can also be ordered to disclose information about the identity of an infringer. [1171]

Both France and the UK also introduced additional legislation targeted at users, which criminalises illegal downloads. This was an answer to the surge in P2P filesharing witnessed in the first decade of the millennium. This will be covered in the following section.

It should also be noted that some Member States chose to regulate NTD requirements for copyright infringements through their national laws. Finland, France, the UK, Spain and Hungary have such regulations in place, while Portugal and Sweden have horizontal NTD statutory requirements which cover copyright.[1172] The Netherlands have a voluntary code of conduct for an NTD system in place.[1173] The nature of the statutory NTD processes varies, with some countries applying it to all intermediaries, while others only cover IAPs or hosting providers. The procedural requirements also vary widely. Since a notice is seen as the principal means for establishing actual knowledge of unlawful content or activity under the ECD, this variety alone is bound to lead to different intermediary knowledge, and hence, liability conditions. The application of intermediary liability rules developed differently for IAPs and different types of hosting providers, with varying consequences for the obligations and liabilities imposed by courts and national statutes.[1174]

b. Enforcement against IAPs – blocking and filtering injunctions

IAPs have very early been in the focus of rightsowners and authorities when it comes to stopping or preventing the availability of copyright infringing material on the internet. Right from the start of the P2P filesharing wars of the early 2000s they were the enforcers of choice of rightsholders against the elusive and distributed architecture of *Grokster*, *eDonkey*,

---

1170 Spindler, 'Präzisierungen Der Störerhaftung Im Internet Besprechung Des BGH-Urteils „Kinderhochstühle Im Internet"' (n 723) 103.

1171 Gila Polzin and Rolf Schwartmann, 'Sharehoster Und Andere Host-Provider' in Thomas Hoeren and Viola Bensinger (eds), *Haftung im Internet: die neue Rechtslage* (De Gruyter 2014) 382.

1172 European Commission, 'SEC(2011) 1641 Final' (n 11) 137–140.

1173 Quintais and Poort (n 1129) 843.

1174 Nicolas Jougleux, 'The Role of Internet Intermediaries in Copyright Law Online Enforcement' in Tatiana-Eleni Synodinou and others (eds), *EU internet law: regulation and enforcement* (Springer Berlin Heidelberg 2017) 285–286.

Kazaa, *The Pirate Bay* and other P2P services.[1175] Their central, gatekeeping position means that they are ideal enforcement targets when it comes to filtering or blocking content unlawfully accessed through or shared by other service providers, such as P2P services, or by private users. At the same time, this technical and infrastructural command has a direct impact on important rights and freedoms. Access to the internet is increasingly regarded as a fundamental right linked to the freedom to receive and impart information and to participate in (the information) society. User traffic data and IP data requested by rightsholders or authorities in the pursuit of illegal downloaders impact the data protection and privacy rights, and for ISPs, the freedom to conduct a business.[1176]

The mere conduit exemption for liability under Article 12 ECD limits IAPs' obligations to the more reactive actions of stopping or preventing infringements following a court or administrative order, which are handed down as injunctions. Rightsholders across the EU, but also worldwide, tried to use these injunctions to oblige IAPs to install systems that would filter or block IP addresses, DNS names, URLs, or data packets, or a combination of these, in order to end copyright infringing activity.[1177] The battles over finding the right balance of the adequate scope of these injunctions took place against the backdrop of the changing technical architecture of P2P services and their business models, and of mounting evidence of infringing use. On the other side, concerns over the impact on fundamental rights by forcing IAPs into potential censorship roles grew in parallel with the importance of the internet and the expansion of its user base. The ECD allows for preventive injunctions against IAPs in Article 12 (3), but prohibits them as soon as they become general monitoring obligations. Meanwhile, IPRED and the Infosoc Directive demand that any inunctions, including against intermediaries, are effective, proportionate and dissuasive.[1178] In addition they must be fair, equitable, not unnecessarily complicated or costly, do not create barriers to trade and provide safeguards against abuse.[1179]

1175 Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 281.

1176 Christophe Geiger and Elena Izyumenko, 'The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking' (2016) 3 American University International Law Review 45, 52–54.

1177 Schmitz (n 30) 546–556.

1178 Directive 2004/48 (IPRED) Article 3 (2); Directive 2001/29 (InfoSoc Directive) Article 8 (1).

1179 Directive 2004/48 (IPRED) Article 8.

National courts have grappled notably with the scope of preventive injunctions. Different approaches with varying outcomes developed out of Member States' jurisprudence. This has been demonstrated as one of the major horizontal challenge in Chapter 3. It is owed to procedural and administrative aspects of injunctions being left to Member States' varying national law and the by now familiar differences in the legal traditions on intermediary law. The CJEU eventually had to step in and give authoritative guidance on the scope of such injunctions by balancing the rights concerned.

The CJEU judgements, despite referring mostly to IAPs, give some useful guidelines in the search for more holistic intermediary responsibilities of hosting providers, where it concerns copyright protection. First, the CJEU specified in its *Promusicae* judgement that Member States are not required to impose an obligation on IAPs that user data be disclosed to rightsholders in order to effectively protect copyright.[1180] This case dealt with a Spanish rightsowner that had asked the ISP *Telefónica de España* to disclose the identities and physical addresses of internet subscribers who had used the P2P filesharing service *Kazaa* in order to exchange copyright protected works. Secondly, *Scarlet Extended* established that a preventive injunction could not oblige an IAP to filter the traffic of all of its customers in order to identify and block file sharing traffic of copyright infringing materials for an unlimited period of time.[1181] Thirdly, in *UPC Telekabel*, although solely basing itself on the Infosoc Directive and not on the ECD, the CJEU allowed an injunction that ordered an IAP to block their customers' access to a website with infringing material, but left the design of the specific measures to the IAP. The IAP would also be freed of any sanctions for breaching the order if it showed that it took all reasonable measures to comply, even when the measures could be circumvented by some users.[1182] Finally, in *Mc Fadden* the CJEU confirmed that a free of charge Wi-Fi hotspot operator could be qualified as an IAP where that service is used for advertising of the goods or services offered.[1183] It was reasonable to expect that such an IAP secured its network against copyright infringing use by installing password protected access.[1184] Requiring users to give up total

1180 *Promusicae* (n 140) para 70.
1181 *Scarlet Extended* (n 139) paras 40, 47.
1182 *Telekabel* (n 757) para 64.
1183 *Mc Fadden* (n 139) para 43.
1184 ibid 99.

anonymity when using the hotspot was deemed a proportionate and effective measure.

The rulings would appear to sketch the contours of a responsibility or duty of care framework within the tight limits of the ECD, IPRED and the Infosoc Directive in the area of copyright. On one side, obliging IAPs to install broad monitoring systems that would cover all user traffic for an unlimited time in the search for copyright infringing material could be seen as disproportional. On the other side, *UPC Telekabel* offered the possibility that an intermediary define the most adequate means for complying with an injunction if this meant that it took all reasonable measures that could be expected of it. It has been criticised that this was a *de facto* outsourcing of fundamental rights balancing exercises to a private entity.[1185] By contrast, it could also be argued that this is a characteristic of a duty of care system. It forces the intermediary to thoroughly consider and weigh the measures it implements, because they are accountable for their decision. It promotes therefore responsible action along the concept of *bonus pater familias* or duty of care,[1186] similar to the "diligent economic operator" standard formulated in in *L'Oréal v EBay* regarding trademarks.[1187] Meanwhile, *Mc Fadden* would vindicate the establishment of processes that seek to establish a user's identity before they join an online network that allows for content downloading and sharing. This appears to be in line with risk management processes that would align the due diligence measures of an actor to the risk of the business model.[1188]

Others have, however, argued that these rulings did little to harmonise intermediary liability provisions in copyright cases.[1189] The cases referred were specific to national legal systems. The consistent delegation of the balancing exercises back to national courts did little to harmonise these provisions, considering the national differences in the nature and application of injunctions.[1190] Meanwhile, as concerns *UPC Telekabel*, some Member States, like the UK, Netherlands or Italy, may not allow for broad injunctions the finetuning of which would lie with the economic operator.

1185 Geiger and Izyumenko (n 1175) 91–92.
1186 Valcke, Kuczerawy and Ombelet (n 551) 109–112.
1187 *L'Oréal v eBay* (n 463) paras 120–124.
1188 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 242–244.
1189 Jougleux (n 1173) 282–286.
1190 Angelopoulos (n 30) 72.

Other countries, like France and Austria, may, however, have less problems in accepting such broad injunctions.[1191]

The enforcement methods against IAPs for illegal file sharing and downloads vary significantly across Member States. In the Netherlands, Spain and the UK for example, injunctions against IAPs to block or remove infringing content are the most commonly used enforcement tools.[1192] The UK stand out as one of the world's most aggressive pursuers of blocking injunctions in the fight against pirate sites. In the UK, the scope of these injunctions has broadened following the *Newzbin* judgement.[1193] They can now cover dynamic injunctions, which target mainly illegal live streaming sites, where URL addresses can be added to the injunctions after the court order has been issued.[1194] In Poland and France, enforcement has focussed on individual users, with France also looking at IAPs to block and filter unlawful traffic. In Germany and Sweden, privately administered cease-and-desist systems appear to be a popular means of enforcement, targeted mainly at users.[1195]

Some EU Member States have introduced administrative enforcement measures, also known as graduated response systems, to go after users who engage in illegal downloading or sharing of content. Enforcement against users means that the IAP is enlisted in helping administrative authorities to pursue infringers at some stages of the process. IAPs are needed to disclose the identity of the IP address subscriber,[1196] issue warning messages and suspend internet access of users who have repeatedly downloaded and shared copyright infringing content, notably through P2P systems.[1197] In

---

1191 Geiger and Izyumenko (n 1175) 92–95.

1192 João Pedro Quintais, 'Global Online Piracy Study Legal Background Report' (Institute for Information Law (IViR), University of Amsterdam 2018) 86–88.

1193 See Chapter 3. *Newzbin* (n 638).

1194 Edwards, 'The Fall and Rise Of Intermediary Liability Online' (n 119) 283–284.

1195 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 85–88. For a detailed description of the cease-and-desist system works in Germany see: Sandra Schmitz and Thorsten Ries, 'Three Songs and You Are Disconnected from Cyberspace? Not in Germany Where the Industry May "Turn Piracy into Profit"' (2012) 3 European Journal of Law and Technology 14.

1196 Usually done through a court order and, following the *CJEU's Promusicae* judgement, only possible where national laws allow for such disclosure in case of copyright infringements. See also: Sandra VI Schmitz, *The Struggle in Online Copyright Enforcement: Problems and Prospects* (1. edition, Nomos 2015) 219–221.

1197 Angelopoulos (n 30) 148.

2006, France proposed its infamous HADOPI Law[1198] which criminalised the acts of illegal file downloading. The obligations imposed on IAPs were outside of the provisions of the intermediary liability framework, but they illustrate the strategic position of IAPs in the online communication chain. In France, it took three years and two legislative rejections before this law was eventually adopted.[1199] HADOPI2 introduces a graduated response system consisting of three strikes against users who illegally download content from the internet. The successive sanctions would lead to a suspension of internet access (a measures which was revoked in 2013) and fines depending on the volume of downloads. The effectiveness of the HADOPI laws has been debated. While the increase in court cases, warning letters and emails appear to have had some impact on the volume of illegal downloads,[1200] there are doubts over its effectiveness. The impact on the general availability of illegal offers remains disputed, while technical circumvention measures continue to evolve[1201] and enforcement costs appear to be high.[1202] Other concerns centre around fundamental rights such as privacy, freedom of speech and the presumption of innocence.[1203] The UK tried to introduce such a graduated response system through the 2010 Digital Economy Act. This was, however, never adopted in its original version. It was eventually watered down into a private warning systems system that allows copyright owners to pursue repeat infringers legally.[1204] A similar private scheme exists in Ireland.[1205]

1198 LOI n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet 2009 (2009-1311).

1199 For a detailed account see : Emmanuel Derieux and Agnès Granchet, *Lutte Contre Le Téléchargement Illégal: Lois Dadvsi et Hadopi* (Lamy 2010).

1200 Quintais, 'Global Online Piracy Study' (n 30) 28.

1201 Schmitz (n 30) 236–240.

1202 Rebecca Giblin, 'Beyond Graduated Response' in Susy Frankel, Daniel J Gervais and New Zealand Centre of International Economic Law (eds), *The evolution and equilibrium of copyright in the digital age* (Cambridge University Press 2014) 86–90.

1203 Derieux and Granchet (n 1198) 195–197. Christophe Geiger, 'The Rise of Criminal Enforcement of Intellectual Property Righs...and Its Failure in the Context of Copyright Infringements on the Internet' in Susy Frankel, Daniel J Gervais and New Zealand Centre of International Economic Law (eds), *The evolution and equilibrium of copyright in the digital age* (Cambridge University Press 2014) 134–137.

1204 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 65.

1205 Gerard Kelly, 'A Court-Ordered Graduated Response System in Ireland: The Beginning of the End?' (2016) 11 Journal of Intellectual Property Law & Practice 183.

Overall, the measures to stop copyright infringement through issuing blocking and filtering injunctions at IAP level can be assessed as showing mixed success. For one, these are mostly reactive measures, which take time, a crucial disadvantage in the internet age, and can be circumvented. Except for the UK, where dynamic injunctions allow for a certain adaptability, especially in the case of illegal live streaming, this is a piecemeal approach. But given the fundamental rights at stake in asking internet gatekeepers to monitor, filter and block content, and disclose user information, judicial oversight is needed. This and the different setup of injunctions within national, legal systems means that the use of IAPs in the fight against copyright breaches varies significantly between Member States. The European Commission sought to clarify the situation through its 2017 Guidance on IPRED. It took note of the fact that some members, namely the UK, Ireland and Belgium, provided for dynamic injunctions through their legal systems. While IPRED did not expressly provide for these measures, it conceded that they can be effective to prevent continued infringements provided they include the necessary safeguards.[1206] That document also clarified that ordering "*excessively broad, unspecific and expensive filtering*" would hit the barriers of Article 3 (1) IPRED, the general monitoring prohibition of Article 15 (1) ECD and applicable fundamental rights. It confirmed and summarised the guidance provided through its case law in *Scarlet Extend*, *Netlog*, *L'Oréal v eBay* and *UPC Telekabel*.[1207]

c. Content hosting, sharing and the road towards primary liability

Hosting providers are the kind of intermediary that third parties use directly to share content. The rise of Web 2.0 was the main trigger for rightsowners shifting attention from IAPs to P2P file sharing services, search engines, social media and UGC platforms. The likes of *The Pirate Bay*, *eMule*, *Grokster*, *Google Search*, *Bing*, *YouTube*, *DailyMotion*, *Instagram* or *Facebook* have enabled an unprecedented surge in interactive, global, mass sharing of images, video and music. Given the economic importance of IP rights, most of the controversies and legal challenges against intermediaries in the fight against unlawful content have been played out in this area. These

1206 European Commission, 'Guidance on Certain Aspects of Directive 2004/48/EC of the European Parliament and of the Council on the Enforcement of Intellectual Property Rights, COM(2017) 708 Final' (n 715) 21.

1207 ibid 20.

rights are exercised by a powerful industry with the money and vested interest in bringing court challenges and in influencing policy. By contrast, defamation and hate speech on the internet mostly concern private parties, which have naturally fewer means to go to court and fight legal battles.

Rightsowners have challenged the legal assumptions on which online platform business models were built: no primary liability due to their intermediary role; an exemption from secondary liability due to their neutral, content agnostic character that relies on third party notifications for stopping unlawful acts.

The national idiosyncrasies that relate to the responsibilities of information hosts under Article 14 ECD in copyright cases will not be recounted in detail here. This section will focus on the role that these actors play in the substance of copyright. This is inevitably linked to some of the challenges to the neutral intermediary status, on the one hand, and the particular characteristics of digital copyright, on the other. It has a resulted in a gradual shift in jurisprudence from allocating secondary liability to finding hosting providers directly liable for copyright infringements. This development will be analysed in the following.

Web 2.0 intermediaries have been challenged in three main areas: unlawful file sharing though P2P systems; hyperlink sharing, mainly through search engines, and content sharing through UGC and social media platforms.

P2P file sharing and hyperlinking

Early file sharing services often boasted their own centralised file index and even hosted content themselves, practices which were early on doomed for failure. The prime example here is *Napster*, whose central file index conferred on it a level of control that made it relatively easy to prove actual or constructive knowledge of infringing activity. The business eventually collapsed when forced to police its content in order to stop infringing use. The crux for the judges was that the service "turned a blind eye to detectable acts of infringement for the sake of profit."[1208] In this US judgement, *Napster's* business model fell under the narrowly applied 'red flag' or wilful blindness standard and was denied protection under the DMCA's

1208 *A&M Records, Inc v Napster, Inc* [2001] United States Court of Appeals for the Ninth Circuit 00-16401, 00-16403, 239 F.3d 1004 [69].

safe harbour. Of course, not every P2P file sharing service derives benefits from infringing activity to the same degree as Napster did. Many of these services have perfectly legitimate uses until today. Still, following this early judgement, file-sharing services, such as *Grokster* or *BitTorrent*, have adapted their architecture and now provide different, unconnected software for tracking and for sharing activities. The idea is that a decentralised and distributed architecture would disperse suspicions over knowledge or control of the service over the data stored or indexed by its users.

At least in Europe this has met with mixed success. In a 2003 Dutch case, P2P software provider *Kazaa* was still cleared from any copyright infringement accusation. The service just provided file exchanging software, which was used for both legitimate and illegitimate acts. Users alone would engage in copyright infringing acts, but not *Kazaa*.[1209] It should be kept in mind that file sharing service providers have been classified as hosting service providers under Article 14 of the ECD. This was confirmed notably by a rush of cases brought against file sharing networks in Germany between 2007 and 2012.

Initially, German courts had found filesharing services secondary liable as interferers for failing to prevent massive copyright infringements that were facilitated by their business models.[1210] They eventually changed this interpretation and applied the jurisprudence developed by the BGH and the CJEU on the liability of online marketplaces as intermediaries under the ECD in a number of so-called *Sharehoster* cases.[1211] This resulted in services like *Rapidshare* or *eDonkey* being charged with proactive duties to prevent the repeated making available of links to infringing content, which the courts recognised as a frequent practice.[1212] This line was confirmed by the BGH in 2012,[1213] with a later qualification that certain sharehoster activities promoted infringing use of their services, through e.g. offering

---

1209 *Vereniging Buma, Stichting Stemra v KaZaA BV* (2003) [2004] E.C.D.R. 16 (Hoge Raad).

1210 *Störerhaftung des Webhosters* [2007] LG Köln 28 O 15/07, MMR 2007, 806; *Rapidshare I* [2008] OLG Hamburg 5 U 73/07, MMR 2008, 823; *Sharehoster II* (n 725).

1211 *RapidShare II* (n 615). German jurisprudence unites all sorts of filehosting and sharing services under the concept of Sharehoster, including cloud services and P2P systems.

1212 ibid 401–402. *Verantwortlichkeit eines Sharehoster-Dienstes für die rechtswidrige Zugänglichmachung urheberrechtlich geschützter Filme* [2010] OLG Düsseldorf I-20 U 166/09, openJur 2009, 1105; see also: Urs Verweyen, 'Grenzen der Störerhaftung in Peer to Peer-Netzwerken' [2009] MMR 590.

1213 *Alone in the Dark* [2012] BGH I ZR 18/11, GRUR 2013, 370.

users anonymity, providing premium accounts for enhanced download bandwidth or loyalty points for users with high amounts of downloads.[1214] Those services would have enhanced verification and infringement prevention duties.

In other Member States, filesharing services were also denied the safe harbour defences under the ECD. In Sweden and Finland, file sharing services *The Pirate Bay* and *Finreactor* lost their safe harbour protection due to the blatantly illegal character of their services.[1215] In Spain, by contrast courts appear to have historically exempted these services from liability either because they saw them as mere software providers or because their activity was protected by the intermediary liability provisions of the ECD.[1216] This trend to assess P2P services as intermediaries was halted by the 2014 CJEU ruling in *Svensson*, which found that hyperlinking was an act of communication and required the author's consent where a new public was being targeted.[1217] Following this judgement, a P2P streaming website was criminally charged for copyright infringements in Spain.[1218] Meanwhile, France has rarely pursued P2P services directly, but chose to go after users or IAPs in the first place.

The *Svensson* ruling was the start of a series of judgements that sought to define different circumstances of hyperlinking on both editorial websites and intermediary sites. In *Bestwater*, *GS Media* and *Filmspeler* the CJEU developed its line on hyperlinking by introducing duty of care elements notably on commercial websites and intermediaries that posted hyperlinks to copyright protected material.[1219] The CJEU confirmed its broad interpretation of the Infosoc Directive Article 3, which eventually offered no alterna-

1214 *Haftung eines Sharehosters als Störer* [2013] BGH I ZR 79/12, ZUM-RD 2013, 565 [32–37]. Polzin and Schwartmann (n 1170) 371–374.

1215 Topi Siniketo, Ulrika Polland and Mikko Manner, 'The Pirate Bay Ruling - When the Fun and Games End' (2009) 20 Entertainment Law Review 12.

1216 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 155–161.

1217 *Nils Svensson and others v Retriever Sverige AB, C-466/12* [2014] EU:C:2014:76 (CJEU) [24].

1218 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 161.

1219 *BestWater International GmbH v Michael Mebes and Stefan Potsch, C-348/13* [2014] EU:C:2014:2315 (CJEU); *GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc, Britt Geertruida Dekker, C-160/15*, [2016] EU:C:2016:644 (CJEU); *Stichting Brein v Jack Frederik Wullems, also trading under the name Filmspeler, C-527/15* [2017] EU:C:2017:300 (CJEU).

tive between primary liability and no liability for intermediaries that posted hyperlinks.[1220]

In the *Pirate Bay* case the CJEU extended the jurisprudence on hyperlinking to P2P filesharing services. The Dutch Supreme Court had called on the CJEU to clarify whether by indexing, categorising and linking to copyright protected works on private users' computers *The Pirate Bay* engaged in an unauthorised communication to the public. The claimant, *Stichting Brein*, a rightsholder association, asked the defendants, IAPs *Ziggo* and *XS4ALL*, to block access to *The Pirate Bay* sites. The IAPs had rejected such blocking injunction on the grounds that *The Pirate Bay* by itself was an online intermediary and therefore not engaged in making protected works available to the public. By applying the methodologies developed in the previous cases, the CJEU found that the P2P sites of *The Pirate Bay* engaged in a communication to the public. Moreover, this activity happened in full knowledge of the consequences – a very large number of torrent files made available works without the authors' consent - and for the purpose of obtaining a profit.[1221] As already done in *UPC Telekabel* and *GS Media*, the CJEU did not consider any liability protections that may have applied to this intermediary under the ECD, unlike in some of the national case law mentioned above. The reasoning of the judgement implies that primary liability for copyright relevant acts excludes the application of the safe harbours for intermediaries under the ECD. The erstwhile condition of actual knowledge for secondary infringements was extended to cover constructive knowledge of infringing acts where the platform had primary liability, at least where P2P platforms are concerned.[1222]

Finally, in 2018 the BGH asked the CJEU directly whether the operator of a shared hosting service engaged in an act of communication according to Article 3 (1) Infosoc Directive by making content accessible to users without rightsholders' consent, if: a) the upload process is automated, b) the conditions of use state that copyright infringing use may not be up-

---

1220 Ansgar Ohly, 'The Broad Concept of "Communication to the Public" in Recent CJEU Judgments and the Liability of Intermediaries: Primary, Secondary or Unitary Liability?' (2018) 13 Journal of Intellectual Property Law & Practice 664, 672–673.

1221 *Stichting Brein II* (n 214) paras 36, 43, 46.

1222 Eleonora Rosati, 'The CJEU Pirate Bay Judgment and Its Impact on the Liability of Online Platforms' (2017) 39 European Intellectual Property Review 16. The platform operators could not be unaware that their service provides access to works published without the consent of the rightholders. *Stichting Brein II* (n 214) para 45.

loaded, c) the operator earns revenue with the service, d) the service is used for lawful purposes, but the operator is aware of considerable concurrent illegal use, e) the service has no search function but third parties post searchable link collections online; f) its renumeration structure incentivises illegal uploads; g) the service offers users anonymity, thus facilitating unlawful behaviour.[1223] Considering the line of argument developed through the preceding cases it appears unlikely that the CJEU will come to another conclusion in this preliminary reference by the BGH.

Despite the aggravated legal environment for certain P2P platforms and their users, places like *The Pirate Bay* continue to exist, partly thanks to their distributed nature and partly due to a host of circumvention technologies available to users.[1224] This puts into doubt whether threatening P2P sites with primary liability will seriously deter intentionally infringing P2P business models.

Search engines, hyperlinking and auto-complete functions

The linking controversy did also influence the liability debate over search engines. In fact, the inefficiency to shut down illegal P2P services led copyright owners to pursue other, more essential intermediaries. After IAP's, copyright owners centred their attention on search engines.

The initial years after the enactment of the ECD were characterised by some confusion over the status of search engines. The CJEU's *Google France*[1225] judgement finally established that search engines were to be seen as hosting providers. At the same time, search engines are intermediaries with a specific functional status. They are essential for the functioning of the internet.[1226] Nevertheless, if the provision of hyperlinks, which is the main means used by search engines of making content accessible, consists of an act of communication to the public, then this would affect their business significantly. Initial jurisprudence over search engines' liability for hyperlinks at national level was divergent, much in line with the unclarity over their status as intermediaries. At one extreme, Belgian and Dutch

1223 *uploaded* [2018] BGH DE:BGH:2018:200918BIZR53.17.0, BeckRS 2018, 26223. Registered as CJEU Referral C-683/18 (Cyando) on 6 Nov 2018

1224 Nicolas P Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019) 98–101; Schmitz (n 30) 556–565.

1225 *Google France v Louis Vuitton* (n 155) para 110.

1226 see Chapter 2

courts found *Google's* search engine directly liable for copyright breaches by posting links to infringing material.[1227] On the other side of the spectrum, a landmark 2003 ruling by Germany's *BGH* freed a news search engine from liability for posting hyperlinks to infringing content. It even significantly limited the service's secondary liability by saying that facilitating the access to works by hyperlinks did not contribute to unlawful behaviour of the party that had made the content available originally.[1228] To complete the disparate picture, a Spanish court in 2007 judged somewhere in between the above extremes. It found that the display of content in search results did breach the copyright of the owners of the referenced website, but that this use was minimal, ephemeral and therefore exempted.[1229] Meanwhile, French courts have ruled conversely. One court accorded *Google's* search engine the protections of the ECD, while yet another one deprived it of these protections.[1230]

As stated above, the CJEU has since had the opportunity to harmonise the interpretation of copyright law regarding hyperlinks. At least the most important search engines by market share as of today, *Google* and *Bing*,[1231] are commercial undertakings that operate for profit. Applying the criteria established in *GS Media* would mean that commercial search engines have duties of care with regards to preventing the publication of hyperlinks to unauthorised content. Any failure to do so would make them primarily liable for making a communication to the public. However, no specific case on commercial search engine liability for copyright content has been escalated to the CJEU as yet. The general uncertainty in this matter is confirmed by Advocate General (AG) *Szpunar's* remark in his Opinion in the *Pirate Bay* case. AG *Szpunar* doubted whether the presumption of knowledge imposed in *GS Media* regarding commercial hyperlink providers

1227 *Copiepresse et al v Google Inc* (n 555). *Technodesign v Stichting Brein* [2004] Court of Haarlem 85489 HA ZA 02-992; Verbiest and others (n 315) 86–90.

1228 *Paperboy* [2003] BGH I ZR 259/00, MMR 2003, 719.

1229 *Audiencia Provincial de Barcelona* [2007] Juriscom.net. in: Cédric Manara, 'Le droit d'auteur contre l'accès à l'information mondiale?' (2011) t.XXV Revue internationale de droit economique 143, para 30.

1230 Manara (n 1228) paras 28–29.

1231 With Google taking 93.2% (91.2%) of the market share in Europe (and worldwide) in April 2020 and Bing 2.9% (2.8%) according to: 'Search Engine Market Share Europe' (*StatCounter Global Stats*) <https://gs.statcounter.com/search-engine-market-share/all/europe> accessed 27 May 2020.

could be applied to indexing sites of P2P networks, which work akin to a search engine.[1232]

The *BGH* may have missed an opportunity for clarification at EU level in the 2017 *Vorschaubilder III* case.[1233] Instead, it went ahead and applied its own modifications to the copyright and hyperlinking jurisprudence of the CJEU. The case concerned the image search functionality of *Google's* search engine. A search service that linked its results to *Google's* image search was accused of making a communication to the public by posting freely accessible thumbnail images (with hyperlinks) on its website. The images were owned by the claimant, a website operator for erotic images. Certain areas of their site could only be accessed and images downloaded by paying users. The *BGH* admitted that in order to avoid primary liability according to the *GS Media* criteria, the search service would need to apply duties of cares by checking whether the targeted material was published without authorisation. However, the *BGH* found that the specific importance of search engines for the functioning of the internet exempted it from these duties.[1234] The operation of commercial search engines would be impossible or seriously hampered if they were obliged to verify the legality of targeted content *ex ante*, given the fully automated nature of internet referencing.[1235] This ties in with the *BGH's* line on search engines in other areas of not manifestly unlawful content, such as defamation and hate speech.[1236] The search service in *Vorschaubilder III* could only be held liable for direct copyright infringement if it failed to act following a notification, which had not been the case. This assessment also appears to make secondary liability for linking intermediaries in copyright superfluous. At least it blurs the borders between secondary and primary liability for search engines, or any hosting providers that post hyperlinks. It confirms a trend of replacing or incorporating secondary or "interferer" liability du-

1232 *Opinion of Advocate General Szpunar, Stichting Brein v Ziggo BV, XS4ALL Internet BV, C-610/15* [2017] EU:C:2017:99 (CJEU) [52].

1233 Ohly, 'The Broad Concept of "Communication to the Public" in Recent CJEU Judgments and the Liability of Intermediaries' (n 1219) 669.

1234 *Vorschaubilder III* [2017] BGH I ZR 11/16, GRUR 2018, 178 [59–60].

1235 ibid 61–62.

1236 *Zur Prüfungspflicht des Betreibers einer Internet-Suchmaschine bei Persönlichkeitsrechtsverletzungen.* (n 949) para 34.

ties into primary copyright, e.g. the communication to the public, at least in German law.[1237]

In France, by contrast, the line on primary liability of search engines in copyright seems to be less clear. *Google Search*, and a number of IAPs, were pursued for the availability of numerous links to streaming sites offering unauthorised content in 2018.[1238] The rightsowners claimed that *Google Search* went beyond the merely passive role that would offer it liability protections under the LCEN. They asked for dynamic de-referencing injunctions that would order *Google* to identify and de-refence on an ongoing basis URLs that led to certain streaming websites with illegal content. The court avoided to go down the thorny route of deciding whether *Google Search* was an active or passive host. Unlike in Germany, it did not find the hyperlinking practices liable for copyright infringement either. Instead it judged that the search engine was merely an intermediary in the sense of Article 8(3) Infosoc Directive. The dynamic de-referencing injunctions were, however, accorded, as they met the proportionality and efficacy criteria demanded of both IPRED and the Infosoc Directive, according to the court.

This judgement was preceded by a 2012 ruling of France's Supreme Court,[1239] which ceded to the demands of the *National Association of Phonographic Publishers (SNEP)* that *Google's Suggest* application stop proposing terms like *Torrent*, *Megaupload* or *Rapidshare* when users searched for certain artists. The Supreme Court struck down a ruling by the Paris appeals court. *Google's Suggest* tool, it said, oriented users systematically to unauthorised copies of works by associating the searches with the disputed terms. This affected the copyright of the authors. *SNEP* had not attempted to engage intermediary or direct copyright liability but rather restricted it-

1237 Ansgar Ohly, 'Keine Urheberrechtsverletzung Bei Bildersuche Durch Suchmaschinen - Vorschaubilder III - Anmerkung von Ansgar Ohly' [2018] GRUR 2018 178, 188 Para 7.

1238 *FNDF et al v Orange, Google et al)* [2018] Tribunal de grande instance de Paris, 3ème chambre 2ème section N° RG 18/10652, (Unreported). See also : 'White Paper Search Engines - Time to Step Up' (Incopro 2019) 63 <https://www.incoproip.com/reports/how-and-why-search-engines-must-take-responsibility-for-tackling-counterfeiters/>.

1239 *SNEP v Google France* [2012] Cour de cassation, Première chambre civile N° 11-20358. See also : 'White Paper Search Engines - Time to Step Up' (n 1237) 64.

self to using intermediary injunctions granted under Article 336-2 of the French IP law.[1240]

Industry analysis has shown that (dynamic) de-referencing injunctions may lead to a significant reduction in traffic to websites that host mainly infringing content. Following a de-referencing injunction against Google in 2011, traffic to sites grouped under the *AllowStreaming* name lost 48.7% of traffic within 5 months.[1241] In France, de-referencing injunctions against search engines have therefore become established practice, with dynamic de-referencing on the line of outcome injunctions being also accepted more recently.[1242] This is of course not withstanding the known means of circumvention, such as the use of VPNs, site mirroring or the use of proxy services, which remain widely effective. Rightsholders in general have also voiced concerns over the administrational burdens and timeliness of injunctions ordered via a court.[1243] Meanwhile, de-referencing injunctions have generally not been granted against IAPs in France.[1244]

There is scarce evidence in the UK of any orders in copyright cases against search engines.[1245] Instead, the Intellectual Property Office (UK IPO) has facilitated a Voluntary Code of Practice on Search and Copyright between *Google*, *Bing* and *Yahoo!* and rightsowner associations.[1246] The parties agree to the delisting of notified URLs leading to infringing content and to focus on automated demotion following notifications. Further technical measures and KPIs to achieve the objectives of reducing the availability of infringing content are to be discussed confidentially between rightsowners and search engines. The agreement also includes work on preventing autocomplete suggestions which lead to infringing material and remove ads from advertisers that profit from linking to this kind of content. The UK IPO supports best practice sharing, research and assessment on

1240 LOI n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.

1241 'White Paper Search Engines - Time to Step Up' (n 1237) 44–47.

1242 *FNDF et al. v Orange, Google et al.).* (n 1237). Outcome injunctions were accepted by the court as proportionate and efficient, while in *APC et autres v Auchan Telecom, Google France et autres* (2013) Unreported (Tribunal de grande instance de Paris). Five years earlier the same court rejected these measures as their proper execution could not be verified by the court and therefore lacked the necessary judicial oversight.

1243 European Commission, 'Summary Response - IPR Enforcement' (n 173) 36.

1244 'White Paper Search Engines - Time to Step Up' (n 1237) 65.

1245 ibid 81.

1246 UK Intellectual Property Office, 'Search Engines and Creative Industries Sign Anti-Piracy Agreement' (*GOV.UK*, 20 February 2017) .

progress. The agreement appears to promote the kind of forward-looking risk assessment needed to effectively fight copyright piracy online. Its significant drawback lies in the fact that it does not appear to be transparent and accountable. It has the hallmarks of a clubby arrangement between dominating industry players to enforce private law provisions, which nevertheless touch on important public interest areas, as provided for in the copyright exception and limitations. It also remains silent on any counterclaims procedures. Although the code allows for the government to impose regulatory action should its objectives not be achieved, there has so far been no official report on its performance.

To cite yet another example of a diverging approach, Spain has created a special safe harbour provision for search engines, outside of, but still similar, to the hosting provider protections of the ECD.[1247]

Whether it concerns primary copyright liability or dynamic (intermediary) injunctions, it appears that search engines enjoy special considerations with courts and legislators due their central status as gatekeepers to internet information. They are thus treated differently to other hosting providers mentioned below. The overall picture is, however, still inconsistent and heterogenic. This is due to, by now, familiar factors: different national legal cultures, uncertainty surrounding both online copyright and online intermediary provisions and different views on how the prevailing problem of infringing material online can be tackled most effectively and proportionally. Overall, the intermediary liability status of search engines remains uncertain to this day.

At the same time, it should not be forgotten that *Google*, which has been dominating the search engine market for years, has continued to operate its own NTD system. According to its obligations under both the US DMCA and the ECD, *Google* has to date delisted over 4.6 billion URLs following notifications by rightsowners.[1248] Until recently, the mechanisms and algorithms that lead to the promotion and listing of certain content, be it sponsored or not, have been hidden deep within the company's realm. This is understandable, on the one side, as this trade secret is key to *Google's* success. On the other side, it leaves users in the dark about why, for example, infringing content is consistently indexed and available through search results. The EU has only very recently introduced regula-

1247 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 49.

1248 Google, 'Content Delistings Due to Copyright – Google Transparency Report' <https://transparencyreport.google.com/copyright/overview?hl=en_GB> accessed 28 May 2020.

tions aimed at bringing more transparency for both business clients[1249] and consumers[1250] into the mechanisms that influence the ranking and display of search results. Maybe enlightenment in this area can also progress our understanding of how search engines can help prevent the display of infringing material in a better way. At the very least, these regulations are proof that commercial search engines are much more than neutral information intermediaries. By imposing these transparency obligations, the regulator has clearly caught on to the fact that these gatekeepers influence, determine and control the appearance of search results.[1251] It will be interesting to see whether and how this helps in defining new responsibilities of search engines in future EU legislation, like the proposed Digital Services Act.

Content sharing platforms

UGC websites and social media platforms have increasingly been in the centre of rightsholders' attention over the last 10 years. The different conclusions over the passive or active role of these intermediaries have been mainly played out in the area of IP rights. In addition to the mounting challenges to the passive status of platforms like *YouTube* or *Facebook*, and the scope of their prospective duties, rightsowners have questioned the role that these actors play in the process of communication to the public. This appears to be in line with the challenges mounted against P2P services or search engines. Actions against P2P platforms were motivated by the massive scale of infringements, the permissive attitude of some of these actors and the evolving jurisprudence on hyperlinking. Search engines were in the line of fire for their central position and the ongoing availability and promotion of links to sites that illegally shared protected material.

1249 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) 2019 (OJ L).

1250 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance) 2019 (OJ L 328). To be discussed in more detail in the sections on trademarks and product safety in this chapter

1251 Pasquale (n 19) 497–503.

For content sharing platforms, rightsholders' motivation can be seen in a more complex set of factors, all related to the characteristics of Web 2.0 interactivity: social media and UGC platforms have increasingly become vertically integrated service providers that compete with established media companies. They profit significantly from content uploaded by users, including unauthorised content.[1252]

It should by now come as no surprise that Member States have tackled this issue in different ways. In Italy, courts have recently charged social media and UGC sites with primary copyright liability. *Facebook* was held liable for communication to the public in 2019 by posting links to content the publication of which was not authorised by the rightsholder. Although the court more specifically considered the lack of due diligence on *Facebook's* side to remove the notified links, it still concluded primary liability by applying the CJEU jurisprudence on hyperlinking.[1253] The same Rome court found the VSP *Dailymotion* directly responsible for infringing material uploaded by its users. The VSP's active role situated it outside the safe harbour of the ECD. *Dailymotion's* ability as an active provider to control content meant it could prevent the publication of unauthorised material, the existence of which it was aware of.[1254]

In Germany, the BGH referred a case to the CJEU that has been pitting a music producer against *YouTube* for over a decade.[1255] The case relates to music works and live performances that were made accessible unlawfully via *YouTube* in 2008. The rightsowner asked *Google* and *YouTube* to remove the files and refrain from publishing any works of its licensee in the future. Months later, works of the artist were again accessible via *YouTube*, which led to the start of proceedings. The case escalated through the German court instances right up to the highest national level. The BGH stayed the case and asked the CJEU whether the defendant, *YouTube,* on whose sys-

1252 Susy Frankel and others (eds), 'After Twenty Years: Revisiting Copyright Liability of Online Intermediaries', *The evolution and equilibrium of copyright in the digital age* (Cambridge University Press 2014) 39–45. Gillespie, 'Platforms Are Not Intermediaries' (n 175) 206; Suzor (n 1223) 19–25.

1253 Rosati, 'Facebook Found Liable for Hosting Links to Unlicensed Content' (n 624).

1254 *Mediaset v Dailymotion* (n 623); Akshat Agrawal, 'THE COPYKAT' (*The 1709 Blog*, 30 July 2019) <https://the1709blog.blogspot.com/2019/07/the-copykat_30.html> accessed 29 May 2020.

1255 *Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 6 November 2018 — LF v Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH (Case C-682/18)* (n 632).

tems copyright protected works were made publicly accessible by users, engaged in an act of communication according to Article 3 of the Infosoc Directive. The *BGH* ties the liability question to VSPs that fulfil a number of criteria that essentially read like definitions of contemporary Web 2.0 platforms: the platform operator earns ad revenue; the upload process is automated and not subject to *ex ante* controls; the VSP receives a worldwide, non-exclusive and royalty-free licence for the uploaded videos; the operator indicates in its terms and conditions that infringing content may not be uploaded; rightsholders are provided with technical tools to block infringing content; for registered users search results are categorised and ranked and certain content is recommended based on past viewing behaviour; after being made aware the VSP removes notified infringing content expeditiously.[1256]

In essence, these questions want to establish whether the characteristics of the new UGC platforms imply a direct involvement in the economic right of communication the public. This direct involvement would then imply the unavailability of the ECD protections. The *BGH* itself is of the opinion that *YouTube* did not have the necessary active knowledge of the availability of the infringing materials.[1257] This is line with German jurisprudence on the role of VSPs and social networks in copyright cases so far, which is by some seen as problematic.[1258] However, in view of the CJEU's broadening interpretation of communication to the public in the hyperlinking cases, especially in *Pirate Bay* case, the *BGH* is unsure whether its view on the liability of the VSP would be in conflict with the lines established by the CJEU. As a side note, it should be pointed out that a Berlin court has recently found the *Amazon* marketplace directly infringing the copyright of product images. The marketplace had assigned product pictures from a perfume brand for which the exclusive license had been given to just one seller, to another seller's offers. This decision by *Amazon* conferred on it the role of a direct infringer, regardless of whether

1256 *Opinion of Advocate General Saugmandsgaard Øe, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc, Google Germany GmbH and Elsevier Inc v Cyando AG, Joined Cases C-682/18 and C-683/18* [2020] EU:C:2020:586 (CJEU) [38].

1257 *Haftung von YouTube für Urheberrechtsverletzungen* [2018] BGH I ZR 140/15, GRUR 2018, 1132 [34].

1258 Matthias Leistner, 'Copyright Law on the Internet in Need of Reform: Hyperlinks, Online Platforms and Aggregators' [2017] Journal of Intellectual Property Law & Practice jpw190, 4–5.

the picture allocation mechanism was automated or not, or whether the pictures were just stored on behalf of a third party.[1259]

With regards to the *BGH's YouTube* referral it should also be noted that, in contrast to the judgement in *The Pirate Bay*, the wilful blindness or permissive attitude towards infringement is not part of the argument.[1260] As will be shown below, *YouTube*, especially, has been spearheading the development of infringement detection software. In its second referred question the BGH asks, whether, if *YouTube* was not engaged in an act of communication, it could still avail itself of the protections of the ECD's Article 14. It seeks more authoritative guidance of the active or passive role of Web 2.0 VSPs. However, CJEU jurisprudence has shown that this assessment is likely to be handed back to the national court.[1261] It should be kept in mind that this reference happened in parallel to the draft and eventual adoption of the DSMD, which created a *fait accompli* of direct liability for content sharing providers for unauthorised uploads by users.[1262] At the final stage of writing this work, the AG published his Opinion on this case on 16 July 2020.[1263] Without going into further detail, AG *Saugmandsgaard Øe* refused to see the activities of *YouTube*, and *Cyando*, the defendant in the second, joined case, as causing primary liability for interference with the right of communication to the public. *YouTube* and *Cyando's* activities consisted of providing mere physical facilities.[1264] The Opinion seems to be critical of the case law developed by the CJEU in *GS Media*, *Filmspeler* and *The Pirate*

1259 *Wiederholungsgefahr, 16 O 103/14* (n 588) para 88. See also Chapter 3

1260 Jurriaan JH van Mil, 'German Federal Court of Justice Asks CJEU If YouTube Is Directly Liable for User-Uploaded Content' (2019) 14 Journal of Intellectual Property Law & Practice 355.

1261 Ansgar Ohly, 'EuGH-Vorlage Zur Haftung Einer Internetvideoplattform Für Urheberrechtsverletzungen - YouTube - Anmerkung von Ansgar Ohly' [2018] GRUR beck-online 1132, 1140.

1262 DSM Directive 2019/790 Article 17 (1).

1263 *Opinion of Advocate General Saugmandsgaard Øe, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH and Elsevier Inc. v Cyando AG, Joined Cases C-682/18 and C-683/18* (n 1255).

1264 ibid 80–88.

Bay.[1265] The AG also rejected a retroactive application of the DSMD to the cases, which would have led to a different outcome.[1266]

The CJEU jurisprudence may have caused uncertainty over the future availability of secondary liability provisions to online UGC platforms and social networks in copyright cases in other EU countries. A 2018 study on global online piracy by *Quintais* indicated that at least for the Netherlands, Poland and Sweden the CJEU rulings may have put into questions previously upheld protections for VSPs and social networks against primary liability for copyright breaches[1267] In Spain, a new law of 2014 introduced new indirect liabilities for copyright infringing acts on online platforms, which may spell out more far reaching liabilities akin to primary infringement.[1268]

To summarise, the interpretations of the availability of the intermediary liability protections in copyright cases has been characteristic of the disparate approaches of EU Member States towards the ECD. National courts showed the same disunity when it came to assessing the role of interactive Web 2.0. hosts in the act of communication to the public. By bypassing the application of the ECD in favour of the Infosoc Directive, the path of secondary liability has been consistently narrowed down for P2P services. Meanwhile, the CJEU has so far provided little clarity with regards to UGC, social media platforms and search engines.

IV. Industry developments: enforcement by private actors

With litigation by copyright owners becoming a constant threat, especially content sharing platforms like *YouTube* became pioneers in developing systems that helped them proactively identify infringing content. Content identification and removal can happen at two stages, during upload by the users, and retroactively, by screening existing content on the site. *Google*

1265 Eleonora Rosati, 'The AG Opinion in YouTube/Cyando: A Regressive Interpretation of the Right of Communication to the Public' (*The IPKat*, 27 July 2020) <https://ipkitten.blogspot.com/2020/07/the-ag-opinion-in-youtubecyando.html> accessed 14 October 2020.

1266 *Opinion of Advocate General Saugmandsgaard Øe, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH and Elsevier Inc. v Cyando AG, Joined Cases C-682/18 and C-683/18* (n 1255) paras 247–250.

1267 Quintais, 'Global Online Piracy Study Legal Background Report' (n 1191) 131, 144, 183.

1268 ibid 49–50, 158.

was the first company that started to develop its own content recognition software. Before discussing *Content ID* and other systems in more detail a short overview over the content identification technologies currently in use on platforms to detect copyright violations will be given. These technologies and systems are, however, not restricted to the detection of copyright infringements. The below discussion will therefore also be exemplary for the general state of play on the use of recognition technologies for the variety of unlawful content discussed throughout this chapter.

a. Content recognition and identification technologies

Fingerprinting

Digital fingerprinting means that a file provided by a rightsowner will be analysed for some defining and unique characteristics using a specific algorithm. The unique characteristics identified by the algorithm may relate to melody lines, frequency or image patterns. The defining features will then be coded into a digital fingerprint which will be deposited in a reference database. For any newly uploaded content files, a digital fingerprint will be created using the same algorithm.[1269] The new fingerprint will then be compared against matches in the reference database. At the same time, existing content on the site may also be screened for matches. Digital fingerprinting, which is at times also referred to as perceptual hashing,[1270] is today the most commonly used technology for copyright motivated content recognition on platforms. It is perceived to be more robust and lighter in its use than other technologies, such as hashing or watermarking.[1271] However, the act of comparison is not perfect. Like any content recognition sys-

1269 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (Conseil Supérieur De La Propriété Littéraire Et Artistique, Centre National Du Cinéma Et De L'image Animée, Haute Autorité Pour La Diffusion Des Œuvres Et La Protection Des Droits Sur Internet 2020) 12–14 <https://perma.cc/4L8X-PBQH> accessed 2 June 2020.

1270 Alper Koz and RL Lagendijk, 'Distributed Content Based Video Identification in Peer-to-Peer Networks: Requirements and Solutions' (2017) 19 IEEE Transactions on Multimedia 475, 475–476. Gorwa, Binns and Katzenbach (n 1066) 4, 7.

1271 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 14.

tem, digital fingerprinting has had difficulties in context sensitive scenarios, where content is subject to exceptions offered by copyright law, such as criticism or parody. In addition, it may be prone to produce errors where content is altered. Its use is further restricted by the fact that a specific fingerprinting method (relying on an algorithm that targets specific content characteristics) will only operate on the particular media to which it has been tailored.[1272]

Several content identification solutions that rely on fingerprinting have been emerging over the last twenty years. Some are proprietary systems developed or bought up by UGC and social media platforms, such as *Google's Content ID*, *Facebook's Rights Manager* tool or *Apple's Shazam*. Prominent free-standing solutions include *Gracenote* in the area of music and audio recognition, and *Audible Magic*, *Signature (by the French National Audiovisual Institute (INA))* or *Vobile* in the area of video and image recognition. As discussed in the section on terrorist content, *Microsoft's PhotoDNA* image and video recognition fingerprinting, or perceptual hashing software, has been mainly deployed to detect child pornographic and terrorist content.[1273] Latest versions of fingerprinting technology also enable the detection of live streaming content.

Hashing

Hashing technology assigns a unique, compressed alphanumerical code to each content file. This technology emerged in the 1950s and has since been available open source.[1274] Contrary to fingerprinting, the algorithm does not analyse features or traits but processes the computational value in its entirety, using cryptography. The result is a unique reference that can only

1272 Engstrom and Feamster (n 741) 14–15.

1273 'How PhotoDNA for Video Is Being Used to Fight Online Child Exploitation | Microsoft On The Issues' (*On the Issues*, 12 September 2018) <https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/> accessed 3 June 2020.

1274 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 26; Hallam Stevens, 'Hans Peter Luhn and the Birth of the Hashing Algorithm - IEEE Spectrum' (*IEEE Spectrum: Technology, Engineering, and Science News*, 30 January 2018) <https://spectrum.ieee.org/tech-history/silicon-revolution/hans-peter-luhn-and-the-birth-of-the-hashing-algorithm> accessed 25 August 2020.

be matched by exactly the same file.[1275] The need for such systems arose during the 2000s when, thanks to the Web 2.0 architecture, file storage started to migrate from individual copies for each user towards distributed storage. The technology has also been used for content identification on P2P networks, although it is increasingly replaced by more adaptable fingerprinting technology.[1276] Platforms and cloud operators increasingly store several copies of a piece of content, by replicating it throughout their architecture. This is done in order to scale access and downloading for a growing number of geographically distributed users.[1277] Hash-matching is useful to enforce stay-down systems that aim to suppress the re-emergence of notified content, be it through re-uploads from outside a platform's ecosystem or by reactivation through (new) links from within its distributed architecture. However, the hash technology cannot deal with variations, however slight they may be. Today it is used by some UGC platforms, like *Dailymotion* and *YouTube*, for stay-down systems following a notice-and-takedown request and in order to supplement existing fingerprinting technology.[1278]

Watermarking

In watermarking, a piece of content is enriched with a digital mark or stamp that will help prevent or track its (unauthorised) use or replication. Different kinds of digital watermarks exist; they may be visible or hidden, embedded in the pixel structure of the file or added as encrypted metainformation that may, for example, identify the creator.[1279] Watermarking is used for a variety of purposes. In the area of copyright protection, it can be used to detect and measure illegal distribution of content. Apart from that,

---

1275 Engstrom and Feamster (n 741) 12–13.
1276 Koz and Lagendijk (n 1269) 475.
1277 Urban, Karaganis and Schofield (n 661) 56–57.
1278 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 26. 'Copyright Protection On Digital Platforms: Existing Tools, Good Practice And Limitations - Report By The Research Mission On Recognition Tools For Copyright-Protected Content On Digital Platforms' (n 734) 17.
1279 Ashish M Kothari, Vedvyas Dwivedi and Rohit M Thanki, *Watermarking Techniques for Copyright Protection of Videos* (Springer Science+Business Media 2018) 4–9.

it is also used to audit the transmission of broadcast content, facilitate document retrieval and for authentication, access and change-tracking of documents.[1280] With regards to IP rights management, watermarking has traditionally been applied by the content creators or rightsowners to ensure that protected content is not replicated, shared or modified without authorisation. In the film industry, the addition of individualised, copy-specific watermarks would allow the tracking of illegally distributed copies back to the original user, thus serving as a deterrent for unlawful distribution or copying. The technique is also used to protect, discover and trace pirated live streams. For example, session-based watermarks that are added by content owners or broadcasters to images or music transmitted during live events, or in a dynamic way during the live stream itself, will help a platform to automatically detect and trace live pirated streams.[1281] Meanwhile, forensic watermarking technology may help protect against screen grabbing from UGC and social media websites by showing visible watermarks to deter this activity or by injecting metadata that helps identify and track the originator.[1282] Online content sharing platforms use watermarking mainly in conjunction with other techniques. For example, fingerprint analysis during an image search enriched with watermark detection adds a second level of security should the former fail to identify a match. However, as a pure content recognition technology, watermarking is not frequently used outside the area of still image recognition.[1283]

Metadata analysis

Metadata is any data that accompanies or surrounds the content in question. The time an image or video was created, its location, version numbers, names of the creator, performers or artists, the file type, file

1280 ibid., Sinha Roy S, Basu A and Chattopadhyay A, Intelligent Copyright Protection for Images, *Intelligent Copyright Protection for Images* (CRC Press 2019) 1–2.

1281 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 28–29. Cleeng, Live Streaming Piracy: Are We Winning This Epic Battle? (2017) 14. <https://cleeng.com/resources> accessed 30 June 2020

1282 Cleeng (n 1280) 15.

1283 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 143.

name, its format, the sample rate etc. are all part of metadata. This data is collected by platforms when content is uploaded to their sites. Usually, certain metadata is required during content upload while other may be optional. Content platforms will require bulk uploaders to include metadata in a structured way in a CSV or XML format during the upload process. The metadata can be normally stored and arranged in various ways.[1284] It would eventually be integrated into the platform's backend data warehouse systems which the company relies on when performing data and business analytics and reporting. Initially, the metadata helps the platform to categorise and structure content. As part of the content or product catalogue, it may also be displayed online. The importance of the catalogue metadata will also be touched upon in the context of due diligence of e-commerce marketplaces in the area of trademark protection and product safety.

For rightsowners, metadata is useful for conducting manual or script-based, automated searches on the database of an online platform or its internal search engine when searching for infringing content.[1285] Platforms may offer rightsholders special access to search their databases by metadata. The results of these searches usually inform NTD request. This technique is ideal when large reams of data need to be analysed quickly, i.e. without the need to compare or analyse the content files themselves. On the downside, this method is prone to inaccuracy. Trivial problems, such as misspellings, shared names, or lacking information may produces false positives or false negatives.[1286] If rightsholders include metadata search results unchecked in notice requests it may result in erroneous takedowns.

1284 Carlos Pacheco, 'YouTube Content ID Handbook - Google' (14 March 2013) 18 <https://www.slideshare.net/carlospacheco74/you-tube-content-id-handbook?from_action=save> accessed 16 April 2021.

1285 This technique was, for example, used by a market surveillance authority in the area of product safety, discussed as part of the interviews in Chapter 5. They had access to the API of the search engine of a major e-commerce marketplace and conducted regular searches for certain illegal products. See also: Engstrom and Feamster (n 741) 11–12.

1286 Bryan Lee, Margarete Arno and Daniel Salisbury, 'Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach' (James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies 2017) 27 7–8. Although this study relates to a different content area, with broader search criteria, it serves as a useful example to demonstrate the high potential error rate when trying to search by metadata on online platforms.

Nevertheless, metadata analysis is in standard use across a variety of platforms, across various content formats.

Predictive analysis

Predictive analysis has already been mentioned in the sections on hate speech and terrorist content. Predictive systems rely on highly automated, sophisticated user and content data analysis that increasingly employ artificial intelligence and machine learning in order pre-empt and prevent unlawful content. This technique incorporates the use of metadata analysis and the data gained through the other analytic techniques described above, as well as the vast amount of data constantly collected by the platform from its users. Predictive analysis also increasingly informs automated detection systems used by online marketplaces to identify trademark infringements and may be key in any system that uses risk-based content analysis and online transaction monitoring, as will be shown in the next section. Due to their central position in the content and, increasingly, infrastructural ecosystem of the internet, the large UGC and social media platforms funnel an ever-growing stream of user, content and infrastructural data through their systems. However, in the area of copyright, predictive analysis has so far been used to a lesser extent compared to other areas. For example, while *YouTube* confirms that the vast majority of its copyright takedowns are automated and detected though its *Content ID* system, this is less due to predictive analysis or artificial intelligence. Their systems rely rather on matching decisions from a reference database, based on advanced fingerprinting technology.[1287]

Predictive analysis centres on the prevention of the first appearance of unlawful content, which is usually difficult if a rightsowner has not officially registered its intellectual property with the platform. Current predictive analysis in the area of copyright violations centres mainly on prioritising processes, such as dispute resolution, automated content analysis or manual decision making in content removal.[1288] For example, predictive analysis can help to focus rightsholder and platform engagement on the most critical cases by concentrating on certain high risk or "red flag" crite-

1287 Gorwa, Binns and Katzenbach (n 1066) 3.

1288 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 52–53.

ria, such as user accounts with sanction histories, certain type of contents (streams), or highly popular and monetised videos.[1289] This is in line with wider fraud prevention activities, which normally use risk-based approaches and also rely on predictive analysis in order to detect and prevent new fraud patterns.[1290]

b. Platform activities addressing copyright infringements – the rise of automated prevention

This more technical explanation has shown that despite their neutral and merely technical hosting functions, modern social media and UGC hosts have at their disposal a sophisticated and wide arsenal of technologies to identify and eventually remove infringing content.

There are several reasons for the rise of automated, preventive copyright enforcement on major platforms today. First, the spectacular growth of content sharing platforms was accompanied by the emergence of major litigations with large rightsholders, such as the *Viacom* challenge in the US, which lasted from 2007 to 2013,[1291] or the previously mentioned battle that pitted *GEMA* against *YouTube* in Germany for over 10 years. Automated enforcement was meant to pre-empt these risks by demonstrating the commitment of the platform to rightsowners concerns, giving them an operational system that allowed them to manage unauthorised content.[1292] Secondly, NTD requests have been growing in line with the amount of content shared through UGC websites. But the automated NTDs that most large platforms have put in place to address this growth rely mainly on metadata searches by rightsholders and are notorious for their inaccuracy and the opportunity they give for abuse.[1293] In addition, their largely unregulated nature in the EU provides for further legal uncertainty. Thirdly,

---

1289 Wang (n 504) 285.

1290 Tricia Phillips, Avivah Litan and Danny Luong, 'Begin Investing Now in Enhanced Machine-Learning Capabilities for Fraud Detection' [2017] Gartner 12; Markus Ruch and Stefan Sackmann, 'Customer-Specific Transaction Risk Management in E-Commerce', *Value creation in e-business management* (Springer 2009).

1291 *Viacom 2013* (n 688).

1292 Gorwa, Binns and Katzenbach (n 1066) 6–7; Leron Solomon, 'Fair Users or Content Abusers? The Automatic Flagging of Non-Infringing Videos by Content ID on YouTube' (2015) 44 Hofstra Law Review 33, 255.

1293 Urban, Karaganis and Schofield (n 661).

automated recognition systems are more scalable to the increasing number of content uploaded. In fact, they will improve as more material is uploaded and the software is trained to learn from mistakes and circumvention attempts. Fourthly, automated recognition tools are fully under the control of the platforms, which can adjust and improve them without outside interference. Notice systems, due to their mandatory nature, are more immediately subject to judicial and regulatory scrutiny. It should come as no surprise, that reporting on the scale and nature of these preventive systems is very limited. Most platforms' copyright transparency reports focus on the content removals that are based on NTD requests.[1294] Lastly, as large online platforms now comprise of extensive information infrastructures, they have access to vast amounts of data. This lends itself to the deployment, training and constant adjustment of content moderation systems. Monitoring and filtering algorithms for unlawful content are but one variety of these encompassing content moderation and information management systems.[1295]

Google's *Content ID* program, rolled out successively since 2007, has probably been one of the most commented and most visible efforts in this area. The system is at the heart of *Google's* copyright management tools. It comprises solutions aimed at more high-volume identifications and takedowns (*Content ID*, *Content Verification Program*), frequent removals (*Copyright Match Tool*) and occasional actions (notice-and-takedown webforms).[1296] Under the *Content ID* program, rightsowners will upload their works to *YouTube* as reference files against which a unique digital fingerprint will be created by *Google* and stored in their database.[1297] The company will screen newly uploaded and existing content for matches with the fingerprint stored in its reference database. If a match is assigned, the rightsowner will be notified and offered to claim the matched content. The uploader will also be informed in case they want to contest the decision made by the fingerprinting technology. By claiming the content, rightsowners have the option of blocking, monetising (gain revenue from ads placed against the content) or simply tracking the use of their content.[1298] The

1294 For example: 'Intellectual Property' <https://transparency.facebook.com/intellectual-property> accessed 8 May 2020.
1295 Gillespie, *Custodians of the Internet* (n 1010) 180–182; Klonick (n 1000) 1664; Sartor (n 236) 19–20.
1296 'Copyright Management Tools - YouTube Help' <https://support.google.com/youtube/topic/9282364?hl=en&ref_topic=2676339> accessed 2 June 2020.
1297 Gorwa, Binns and Katzenbach (n 1066) 6.
1298 Carlos Pacheco (n 1283).

Content Verification Program allows rightsowners to search manually for content that infringes their rights through a metadata search and then submit (bulk) notices. Meanwhile, the *Copyright Match Tool* allows uploaders to perform the functions of the *Content ID* system on an ad-hoc basis. They will need to choose individually the course of action if an allegedly infringing video is identified (do nothing & track, block or monetise).

As of today, the *Content ID* database has over 80 million reference files deposited by those rightsowners who cooperate with the world's largest VSP.[1299] Meanwhile, *YouTube* has continuously improved the performance of its tool, adapting its technology, amongst others, to the hosting of live streams, exclusive broadcasting or music channels. It also diversified its service offers to rightsowners. For example, rightsowners may create reference files without uploading the actual content to the platform. In conjunction with the monetisation offer, which has aptly been identified as a stroke of genius,[1300] the company could cash in on additional ad revenue where rightsholders choose to keep content online. In the end it is against *YouTube's* commercial interest to remove content, as it is the broad selection of videos that drives traffic and generates revenue. At the same time, *YouTube* managed to pacify and buy-in rightsowners by offering quick and effective, although possibly less lucrative IP exploitation, in exchange for the bitter pill of them relinquishing some of their rights to the platform. This difference in compensation between what rightsowners have gained through the monetisation and copyright enforcement programs from platforms, and what they allegedly could have earned through traditional licensing agreements, is also called the "value gap." The "value gap" has become a major argumentation tool of rightsowners to push regulators into imposing more far reaching responsibilities on platforms when it comes to policing infringing content online.[1301]

As of 2018, 98% of *YouTube's* copyright claims had been made via its *Content ID* system. In 2017, 98% of *Content ID* claims were fully automated, which means the works were automatically identified and the rightsholders' preferred actions automatically applied to the claimed content. In 90% of cases the rightsowners chose to monetise the content, therefore

1299 'How Google Fights Piracy' (Google 2018) 25 <http://services.google.com/fh/files/newsletters/how_google_fights_piracy.pdf> accessed 2 June 2020.

1300 Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 275.

1301 European Commission, 'COM(2016) 288 Final' (n 223) 8–9.

leaving it on the site.[1302] Considering that to date over 800 million videos[1303] were claimed through *Content ID*, and this represents 98% of all copyright issues, then the company has still had to process over 16 million (i.e. 2%) non-automated requests in the form of notices since 2007. This also means that the statutory NTD procedures, anchored in the US American DMCA) and the European ECD, although sizeable, account for but a small part of copyright motivated content removals. Major rightsowners are now the trusted flaggers (called partners under the *Content ID* program) and notice providers whose requests are expedited. *YouTube* claims to have handed out $3 billion worth of revenue from content monetisation to rightsowners over the last 5 years under this program.[1304] The automated processes that have emerged out of the cooperation between (global) entertainment and media industry players and major platforms rule the world of copyright enforcement today. *YouTube* set the pace for similar efforts of other content sharing providers in this area.

The VSP *Dailymotion* employs automated content recognition since 2007. France-based *Dailymotion*, one of the few European UGC platforms with a global significance, has also been involved in a number of litigations concerning copyright infringements, chiefly in Europe. It has, however, relied mainly on external market solutions, using *Audible Magic* for music recognition and *INA-Signature*, developed by the French *National Audiovisual Institute (INA)*, for video recognition. It has recently also been developing its own content protection system that scans content uploaded by participating rightsowners against the database of its two external providers.[1305] In addition, it allows qualifying rightsowners ("Partners"), to monetise claimed content, similar to *YouTube*.

The *AudibleMagic* fingerprinting technology for audio and video is reportedly also used by *Facebook, Twitch, TikTok, Vimeo or Vkontake*, with notably *Facebook/Instagram* and *Vimeo* developing their own tools for rightsowners to manage (block or monetise) content for which they have claimed copyright.[1306]

1302 'How Google Fights Piracy' (n 1298) 24–25.

1303 'Press - YouTube' (n 668).

1304 'How Google Fights Piracy' (n 1298) 25.

1305 'Protect Your Copyright with Fingerprints' (*Dailymotion Help Center*) <http://faq.dailymotion.com/hc/en-us/articles/203921173> accessed 4 June 2020.

1306 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 30-31,; Urban, Karaganis and Schofield (n 661)

Music sharing platform *Soundcloud* has been using *Audible Magic's* sound recognition services, but developed its own solution as of 2012. Again, uploaded content will be screened against a fingerprint database during upload and at a number of intervals thereafter.[1307]

For other larger players, such as *LinkedIn*, *Twitter* or *Snapchat* it is not known whether they use fingerprinting recognition tools in the fight against copyright infringements.[1308] Meanwhile, the market for content recognition technologies and services has seen a constant growth and diversification in providers and service offers.[1309] This is not only owed to platform demand but also due to increasing demand from rightsholders to protect their IP assets on the internet.

Little is, however, known of the practices of smaller content sharing platforms in the market. A 2016 study conducted in the US has shown that smaller platforms that rarely receive copyright claims would run manual NTD processes initiated by rightsowners through webforms. Medium-sized players were gradually moving towards automated webforms that allow for bulk notice submissions. They would eventually feel pressurised by rightsholders to move into automated recognition systems that allow for privileged access by larger content owners.[1310] But these systems require substantial investment and architectural choices that go beyond just integrating an API for rightsowners. *Google* spent reportedly up to USD100 million in developing and maintaining its *Content ID* solution.[1311] *SoundCloud*, a much smaller player, invested between EUR5 – 10 million for developing (just) its sound recognition tools. It employs 12 full time staff

---

59; 'Copyright Management | Facebook' <https://rightsmanager.fb.com/> accessed 4 June 2020; Gorwa, Binns and Katzenbach (n 1066) 6.

1307 European Commission, 'Commission Staff Working Document - Impact Assessment - Assessment on the Modernisation of the EU Copyright Rules Accompanying the Documents Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market and Proposal for a Regulation of the European Parliament and of the Council Laying down Rules on the Exercise of Copyright and Related Rights Applicable to Certain Online Transmissions of Broadcasting Organisations and Retransmissions of Television and Radio Programmes - SWD(2016) 301 Final - Part 3/3' (European Commission 2016) 166.

1308 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 32.

1309 ibid 16–19; European Commission, 'Impact Assessment 3/3 - DSM Directive' (n 1306) 167–172. for an overview of current service providers.

1310 Urban, Karaganis and Schofield (n 661) 71–73.

1311 'How Google Fights Piracy' (n 1298) 27.

consisting of engineers, product managers and NTD agents to run the system.[1312]

Overall, the landscape of copyright enforcement on platforms is still uneven. However, there is a marked trend of large UGC and social media platforms to move towards automated enforcement through the deployment of content recognition.[1313] The pressure of rightsholders in this game is not negligible. The trend indicates a move clearly beyond the obligations that are currently required by the intermediary liability provisions in the ECD (and the DMCA). In fact, it has been argued that

> *"in a technical sense the law still governs, but over the last decade sites like YouTube have begun using software (named "Content ID") to intelligently and proactively take down copyrighted works. This understanding, implemented in code, was undertaken in the shadow of the law, but it is not compelled by it, and the decisions made by the software are now more important than the law."*[1314]

Meanwhile, smaller players are less likely to be able to support nor necessarily require these automated tools.

While content recognition technologies may become increasingly robust and accurate,[1315] there remain problems.[1316] First, while the technology maybe good at identifying matches, it may be less so when deciding on infringements.[1317] A video or song that is matched to a fingerprint on a

---

1312 European Commission, 'Impact Assessment 3/3 - DSM Directive' (n 1306) 166.

1313 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 3; Urban, Karaganis and Schofield (n 661) 71–73.

1314 Tim Wu, 'Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems' (2019) 119 Columbia Law Review 2001, 2007.

1315 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 3.

1316 European Commission, 'Commission Staff Working Document - Impact Assessment - Assessment on the Modernisation of the EU Copyright Rules Accompanying the Documents Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market and Proposal for a Regulation of the European Parliament and of the Council Laying down Rules on the Exercise of Copyright and Related Rights Applicable to Certain Online Transmissions of Broadcasting Organisations and Retransmissions of Television and Radio Programmes - SWD(2016) 301 Final - Part 1/3' (European Commission 2016) 140–141.

1317 Gorwa, Binns and Katzenbach (n 1066) 8. Engstrom and Feamster (n 741) 18–19.

platform's internal database may still legitimately be shared due to copyright exceptions. It may be a parody, scientific citation, criticism or part of a news report. Automated systems are (still) notoriously imperfect in detecting these often context-sensitive scenarios. Artificial intelligence and predictive analysis, although used for hate speech and terrorist content, and heavily researched, are not yet developed enough to make these decisions with a high level of accuracy in the area of copyright.[1318] Failure to respect these exceptions has been widely commented on and is a major drawback of these systems as of today. It may negatively affect cultural diversity, user rights and freedom of expression.[1319] Secondly, the decision-making procedures and appeals processes are unclear and deeply hidden within the organisational structure of these platforms. Transparency on NTD procedures is already a challenge, but detailed transparency reporting in the area of automated content decision-making is even harder to come by. This is not surprising, since the automated tools deployed by platforms rely on agreements with rightsowners and their associations, which may have an interest to conceal their engagement with platforms from public scrutiny. If, for example, automated tools pick up *en masse* on uploads subject to legitimate copyright exceptions, then Google notifies the rightsowner and it is eventually up to them to 'choose' whether they respect or violate these exceptions. At the same time, users often remain unaware of their rights to oppose takedowns or simply fear litigation by major rightsholders.[1320] Thirdly, this means that the original copyright wars between rightsholders changed into an "accommodation between dominant incumbents."[1321] This, however, may create entry barriers on both sides: smaller platforms that may not be able to attract content from larger rightsholders due the inability to guarantee the same level of automated rights protection; smaller, individual artists may not get access to the same protection

1318 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268) 48–58.

1319 See for example: Solomon (n 1291) 257–259; Sabine Jacques and others, 'The Impact on Cultural Diversity of Automated Anti-Piracy Systems as Copyright Enforcement Mechanisms: An Empirical Study of YouTube's Content ID Digital Fingerprinting Technology' 287–288 <http://rgdoi.net/10.13140/RG.2.2.14443.54560> accessed 5 June 2020; Erickson and Kretschmer (n 1134).

1320 Solomon (n 1291) 253.

1321 Urban, Karaganis and Schofield (n 661) 125.

measures as large rightsowners,[1322] while UGC uploaded by individuals may face a higher risk of being flagged for infringements.[1323]

Nevertheless, automated copyright enforcement, for all of its problems, is not only going to stay, but to grow further in importance. Courts have already been pricing this into their judgements when ruling on the obligations of intermediaries. As an example, German judges in the *GEMA v YouTube* court saga have successively obliged *YouTube* to use its *Content ID* software, supplemented by word filters, where needed, to prevent the re-upload of previously notified infringing content.[1324] In a previously mentioned recent Italian case against *Dailymotion*, a Rome court took the existence of filtering software on the part of the platform as a justification for imposing an obligation to use that technology for preventive monitoring.[1325] In that context, the constant advance in automated filtering and content identification technologies implicitly raises the minimum knowledge standards that can be applied to evaluate the liabilities of intermediaries. This may eventually bring it in conflict with the ECD's Article 15, which imposes a ceiling by prohibiting general monitoring obligations, which in itself is an unclear concept and has been differently interpreted.[1326] For example, some have argued that online platforms have for some time been able to monitor and surveil virtually everything a user does on their platforms and the internet in general.[1327] The picture is further complicated in copyright by the fact that primary liability has been brought into play for intermediaries, which will only spur the use of automated content filtering.

V. EU legal initiatives – the Digital Single Market Directive (DSMD)

The European Commission had identified copyright early on as an area where intermediary liability provisions led to differing legal interpreta-

1322 ibid 139.
1323 Solomon (n 1291) 238–239.
1324 *GEMA v YouTube* (n 264) 407. This line was confirmed in various successive cases opposing the two parties in Germany, See also: Angelopoulos (n 30) 158.
1325 *Mediaset v Dailymotion* (n 623); Gentile (n 623).
1326 Angelopoulos (n 30) 278–279.
1327 For example: Friedmann (n 16); Zuboff (n 5).

tions, and disparate and ineffective enforcement.[1328] Although it did not see a need to amend the horizontal framework of the intermediary liability exemptions under its 2015 Digital Single Market policy, it still identified a number of content areas that required special attention. As part of its new "sectoral, problem driven approach to regulation" it announced a copyright package aimed at a "fairer allocation of value generated by the online distribution of copyright-protected content by online platforms."[1329]

This resulted in the DSMD,[1330] which came into force in June 2019, following a lengthy, passionate and highly publicised negotiation process. Member States will need to transpose it into national law by 7 June 2021. The debate during the drafting phase of the DSMD exposed the substantial lobbying efforts of the various stakeholder groups - the entertainment and music industry, online intermediaries and civil society - in the law-making process. This is a vivid expression of the immense commercial and public interest that digital copyright musters in today's information society. The original draft of the Commission, first presented in 2016, was changed several times in intense discussions between the Commission, the Council and the European Parliament.[1331]

The finally adopted version, still highly criticised,[1332] attempts to solve the intermediary liability problem of online OCSSPs by making them directly liable for copyright relevant acts of communication to the public or

1328 Van Eecke and Truyens (n 316) 20–26. European Commission, 'SEC(2011) 1641 Final' (n 11) 40; European Commission, 'Summary Response - IPR Enforcement' (n 173) 45–48.

1329 European Commission, 'COM(2016) 288 Final' (n 223) 9. Apart from copyright The European Commission also announced to review the AVMSD in the area of hate speech and child protection, the need for formal NTD procedures and to provide guidance on voluntary measures of platforms.

1330 DSM Directive 2019/790.

1331 For summary overview of the different positions of the EU negotiating parties and their evolvement see: Cole, Etteldorf and Ullrich (2020) (n 17) 140–143. Also: João Quintais, 'The New Copyright in the Digital Single Market Directive: A Critical Look' [2020] European Intellectual Property Review 2–3. CREATe, 'EU Copyright Reform: Timeline of Developments & Comparison Table' (*UK Copyright and Creative Economy Centre University of Glasgow*) <https://www.create.ac.uk/policy-responses/eu-copyright-reform/#table> accessed 5 October 2020.

1332 For example by: Gerald Spindler, 'The Liability System of Art. 17 DSMD and National Implementation – Contravening Prohibition of General Monitoring Duties?' (2020) 10 JIPITEC <https://www.jipitec.eu/issues/jipitec-10-3-2019/5041>; Quintais, 'The New Copyright in the Digital Single Market Directive' (n 1330).

of making available to the public.[1333] It leaves, however, open the still existing ambiguities regarding search engines, and to some extent, P2P platforms. To dispel any doubt over the primary liability imposed on OCSSPs, the DSMD clarifies that these services would lose the intermediary immunities offered in Art. 14 (1) ECD. This appears to be a continuation of the CJEU's jurisprudence in hyperlinking, which introduced the view that intermediaries could be directly liable for copyright relevant acts.[1334] As for the type of providers concerned, OCSSPs are defined as ISSPs which store and give public access to a large amount of copyright-protected works uploaded by its users.[1335] In addition, these services organise and promote the protected content for profit-making purposes. Promotion in this sense would not refer to the promotion of the content in question, but rather the placing of advertisements next to protected content.[1336] This wording implicitly acknowledges the active role of OCSSPs, which makes their removal from the ECD's Article 14 (1) immunities logic. The bulk of UGC platforms, *YouTube*, *Dailymotion*, *Vimeo* and *Facebook*, which have been in the line of fire of rightsholders, would find themselves outside the intermediary liability privileges of the ECD. This follows the argument that, as primary infringers that make works publicly available, they have clearly departed from being passive and merely technical intermediaries. The DSMD is therefore different from the AVMSD and the TERREG proposal, which maintain the application of the intermediary liability exemption conditions of the ECD and therefore the assumption of neutral intermediaries. Instead, these latter provisions attempt to establish enhanced responsibilities within the framework of the ECD.

The analysis could stop here, because under the DSMD, OCSSPs are not part of the current intermediary liability framework any longer, and potential primary infringers. But this view would stop short of the fact that even though active, they remain intermediaries in that they share content originally uploaded by a third party, the originator, and the user who downloads and accesses it. As this work will attempt to explore an alternative intermediary liability framework which does away with the active/passive distinction of the current ECD, the DSMD remains of interest. The DSMD

1333 DSM Directive 2019/790 Article 17 (1).

1334 Rosati, 'The CJEU Pirate Bay Judgment and Its Impact on the Liability of Online Platforms' (n 1221) 15. Nordemann (n 1160) 26.

1335 DSM Directive 2019/790 Article 2 (6).

1336 Spindler, 'The Liability System of Art. 17 DSMD and National Implementation – Contravening Prohibition of General Monitoring Duties?' (n 1331) 346.

also acknowledges this special intermediary (liability) situation[1337] by imposing specific obligations that would protect OCSSPs from being liable as primary infringers. This has led to controversy over the status of Article 17 DSMD, notably whether this Article is *lex specialis* to both the ECD and the Infosoc Directive or not.[1338]

OCSSPs have two alternative obligations. First, the platforms concerned will need to get the authorisation from rightsholders for sharing copyright-protected content. This could be done through the conclusion of licensing agreements.[1339] As stated above, the relations between incumbent OCSSPs and major content owners have been warming up over the last decade, with notably *YouTube* and *Facebook*[1340] signing major licensing deals in this area. The large OCSSPs are therefore in a markedly more comfortable position than smaller players. The DSMD may even entrench their dominant market position.[1341] Licensing agreements, especially where it concerns multi-territorial rights, can be lengthy and complicated to negotiate. It remains open, whether smaller platforms would have enough leverage to attract the interest of large rightsholders to step into such agreements. Even larger platforms may not be able to obtain authorisation for each and

1337 DSM Directive 2019/790 Recital 66.

1338 The view that Article 17 is *lex specialis* is held by: Martin Husovec and João Quintais, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms' (Social Science Research Network 2019) SSRN Scholarly Paper ID 3463011 <https://papers.ssrn.com/abstract=3463011> accessed 1 September 2020. Nordemann & Waiblinger oppose this viewpoint: 'Art. 17 DSMCD: A Class of Its Own? How to Implement Art. 17 into the Existing National Copyright Acts, Including a Comment on the Recent German Discussion Draft - Part 2' (*Kluwer Copyright Blog*, 17 July 2020) <http://copyrightblog.kluweriplaw.com/2020/07/17/art-17-dsmcd-a-class-of-its-own-how-to-implement-art-17-into-the-existing-national-copyright-acts-including-a-comment-on-the-recent-german-discussion-draft-part-2/> accessed 5 October 2020.

1339 DSM Directive 2019/790 Article 17 (1).

1340 Chris Welch, 'Facebook Now Has Music Licensing Deals with All Three Major Labels' (*The Verge*, 9 March 2018) <https://www.theverge.com/2018/3/9/17100454/facebook-warner-music-deal-songs-user-videos-instagram> accessed 9 June 2020; Brad Spitz, 'France: YouTube, Universal and SACEM Enter into a New Agreement' (*Kluwer Copyright Blog*, 16 April 2013) <http://copyrightblog.kluweriplaw.com/2013/04/16/france-youtube-universal-and-sacem-enter-into-a-new-agreement/> accessed 9 June 2020.

1341 'Why Tech Giants Have Little to Lose (and Lots to Win) from New EU Copyright Law – Maurizio Borghi' (*Inforrm's Blog*, 19 September 2018) <https://inforrm.org/2018/09/20/why-tech-giants-have-little-to-lose-and-lots-to-win-from-new-eu-copyright-law-maurizio-borghi/> accessed 8 June 2020.

every piece of content considering the sheer volume of works on their systems. On the other side, smaller rightsowners, such as independent artists, labels or producers, may just not be a priority of large platforms for negotiating an agreement, although this could be a litmus test for assessing best effort of platforms to obtain such an authorisation.

This leads to the second option for avoiding liability. OCSSP are required to demonstrate that they have undertaken best efforts in: obtaining an authorisation from rightsowners; preventing the availability of unauthorised content by applying "high industry standards of professional diligence" after having received information on specific protected works by rightsowners; remove works expeditiously after receiving a notice from a rightsholder and ensure removed works are not uploaded again (stay-down obligation).[1342] The best efforts are to be assessed in view of the OCCSP's size, its particular business model, the type of works uploaded by users and the resources at its disposal in order to prevent unlicensed content.[1343] Although not mentioned explicitly, the passage requiring preventive efforts based on high professional diligence standards implies that platforms will likely need to use automated filtering systems, or upload filters, in order to prevent unauthorised content on their sites. As demonstrated, most large OCSSP now use these automated recognition systems. The DSMD's impact assessment and other public studies have been eager to demonstrate that the market for content recognition has diversified, with a variety of technology providers emerging over the recent years.[1344] This could be interpreted as furnishing a justification that, first, OCSSPs have the choice to acquire such technology as part of their best efforts, and, secondly, the technology constitutes a high industry standard of professional diligence. The fact that the Commission tries to establish best practices with regards to these standards through industry stakeholder fora by considering market developments in the technology only reinforces this view.[1345]

1342 DSM Directive 2019/790 Article 17 (4).

1343 ibid Article 17 (5).

1344 European Commission, 'Impact Assessment 1/3 - DSM Directive' (n 1315) 140–142; European Commission, 'Impact Assessment 3/3 - DSM Directive' (n 1306) 164–172 Annex 12A; 'MISSION REPORT: Towards More Effectiveness of Copyright Law on Online Content Sharing Platforms : Overview of Content Recognition Tools and Possible Ways Forward' (n 1268); 'Copyright Protection On Digital Platforms: Existing Tools, Good Practice And Limitations - Report By The Research Mission On Recognition Tools For Copyright-Protected Content On Digital Platforms' (n 734).

1345 DSM Directive 2019/790 Recital 71.

The DSMD introduces an exemption, by which start-up platforms will wholly or partly be exempted from these requirements.[1346] In addition, assessing best efforts in the context of the OCSSP's business model, the type of content hosted and the resources available, makes for a certain degree of flexibility that would allow smaller OCSSP to scale their efforts by e.g. using a risk-based approach: an OCSSP could identify the content categories or types of content that are at the highest risk of being used for copyright infringements and concentrate its efforts on these. The DSMD also enshrines respect for copyright exceptions into OCSSPs best efforts and obliges them to put in place effective complaints and redress mechanisms. Whether, however, the general monitoring prohibition, taken over from Article 15 ECD will provide additional protection is questionable, especially since that term remains undefined.[1347] Courts and experts may still discuss in years to come whether "best effort" content recognition results in general monitoring or not, while a more useful discussion would rather define criteria for a proportional use of such technology.

Article 17 DSMD essentially requires that OCSSPs act as diligent economic operators. Compared to the ECD, these are the kind of enhanced responsibilities that maybe justified considering the activities and functionalities of today's UGC and social media platform and their effect on copyright. However, the DSMD lacks a solid procedural and supervisory framework to ensure a proportionate and accountable implementation of the enhanced obligations imposed by Article 17. The determination of OCSSP's best efforts must be made according to transparent criteria, especially where it concerns the use of content recognition technology and respect of user rights. Facilitating discussions on best practices through stakeholder dialogues and issuing guidance notes are unlikely to be enough to achieve adequate respect of copyright exceptions, rights of redress and complaints as part of OCSSPs best efforts.[1348] Concerns over the respect of these rights during implementation and operation of Article 17 are therefore more than justified.[1349] These concerns also play a role in the ongoing judicial challenge of the DSMD brought by the Republic of Poland, which is cur-

1346 ibid Article 17 (6).
1347 ibid Article 17 (8).
1348 ibid Article 17 (7), recital 70.
1349 João Pedro Quintais and others, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' (2020) 10 JIPITEC.

rently pending before the CJEU.[1350] Poland seeks to annul Articles 17 (4) (b) and (c) of the DSMD, because it thinks that the best efforts required from OCSSPs that have failed to get an authorisation from rightsowners will inevitably lead to the use of upload filters. This would result in an undue interference with the rights to freedom of expression and to receive and impart information as guaranteed by Article 13 CFREU.

While the AVMSD tasks ERGA with overseeing and facilitating the implementation of proportionate and transparent proactive measures and provide technical expertise and advice on platforms' preventive obligations towards hate speech,[1351] such a co-regulatory setup is missing in the DSMD. As has been demonstrated previously, purely self-regulatory best practice sharing initiatives have so far created little momentum towards achieving transparent and equilibrated outcomes in respect of due process, especially for users. They are ill suited to shed light on both the mandated licensing practices between market incumbents and the largely opaque content filtering and takedown responsibilities.

VI. Summary and outlook

In copyright, the enforcement of intermediaries' liability framework evolved in the patchwork manner that is characteristic of the various national secondary liability (exemption) approaches, different sanction regimes under national copyright, ordinary law rules and, at times, supplementary sectoral legislation. None of the regimes that have emerged did manage to contain the widespread occurrence of copyright infringements that accompanied the rise of Web 2.0 intermediaries and user interactivity. Due to the particular nature of copyright, the activities of modern online platforms increasingly raised questions on substantive copyright aspects, such as the communication to the public. Many national courts, incensed by the CJEU, have concluded that primary liability is a justifiable verdict where it concerns P2P file sharing services, UGC sites and social media platforms that share large amounts of content. The situation is still less clear for search engines, due to their essential role in the working of the internet.

1350 *Action brought on 24 May 2019 — Republic of Poland v European Parliament and Council of the European Union, C-401/19* (CJEU). The judgement in this case is not expected before spring 2021.

1351 AVMSD 2018/1808 Article 30b, Recital 58.

The imposition of primary liability on OCSSPs through the recent DSMD means that the ECD will now cease to be applicable for an important group of online platforms in the future, at least where it concerns copyright. Direct liability will undoubtly provide a larger stick against platforms to prevent unlawfully shared content. The enhanced responsibilities formulated by the EU lawmaker may arguably be proportionate to the role these actors play in the exchange of protected content and in user interaction. Many of the large and dominating actors are already monitoring and filtering content systematically. In fact, most of their content takedowns happen according to proactive, automated systems. They have stepped into licensing agreements with major rightsowners or their licensing organisations. However, the way the new obligations are being formulated may reinforce relationships between incumbent rightsholders and dominant platforms, and eventually throttle competition, freedom of speech and variety of content. Meanwhile, the best efforts in preventing unauthorised content, which platforms need to demonstrate where they did not receive an authorisation, are fraught with potential pitfalls. They lack solid regulatory oversight and transparency requirements that would ensure respect of user rights and public interest copyright exceptions during the use of filtering technologies and notice-and-stay-down procedures.

As regards P2P sites, despite the clamp down on these intermediaries, there remain ample circumvention and avoidance techniques available for determined infringers. Here, the answer against unlawful activities in the area of copyright would probably lie more in the creation of viable, affordable and widely accessible legal offers as well as better global coordination.

The aggravating stance against intermediaries has even gripped more unlikely jurisdictions. The US Government recently published the results and recommendations of its multi-year study on the intermediary liability framework under the DMCA.[1352] These recommendations hint at a significant rethink of intermediary liability protections for copyright infringements. They confirm that the critical elements of the ECD outlined in this work are also a concern for the policymakers of the DMCA's section 512. The US Copyright office suggests a review of the eligibilities of the safe harbour defence for today's hosting providers, with a possibility to create specific passages for P2P systems and payment service providers. Other recommendations include legislation to make repeat infringer policies mandatory, provide legal clarifications of the actual knowledge and wilful blindness standards, impose higher penalties for abusive notices, clarify the

1352 'Section 512 of Title 17 - A Report of the Register of Copyrights' (n 409).

timeframes for expeditious removal and facilitate voluntary initiatives in infringement prevention by supporting the development of technical standards.[1353] It even states that the progress made in fingerprinting technology may make this technology ubiquitous and feasible for all online service providers in the future.[1354]

5. Trademarks

I. Trademarks, counterfeiting and e-commerce

The rise of online marketplaces on the commercial web has opened new opportunities for consumers to choose from an unprecedented variety of goods, at a global level, and often at competitive prices. It has also created new business opportunities for small and innovative businesses around the world, transformed supply chains and uprooted traditional retail markets. Like in any other area of the internet, this rise has also opened the door for unlawful and criminal activities. The sale of trademark infringing goods, be they counterfeits, unlawful imitations or grey goods, but also illegal or unsafe products, although an ancient phenomenon, has been facilitated by online marketplaces and the internet in general.[1355] Estimates show that already in 2003, the value of counterfeit goods traded online amounted to $25 billion.[1356] More recent data is hard to come by due to the evasive nature of this illicit activity. Evidence remains therefore largely anecdotal. The pharmaceutical company *Pfizer* reported that between 2015 and 2018

1353 ibid 2–7.

1354 ibid 178.

1355 Agreement On Trade-Related Aspects Of Intellectual Property Rights (TRIPS) 1994 Article 51, fn 14. Defines counterfeited goods as "*…any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark…*" Counterfeit goods are also more colloquially referred to as fake goods. Grey goods are goods that although authorised for sale, are marketed through distribution channels for which the rightsholder has not provided an authorisation to the distributor. Grey or parallel imports refers to products for which the rightsowner has given no authorisation that they be imported into the jurisdiction.

1356 'The Economic Impact of Counterfeiting and Piracy OECD - Executive Summary' (OECD 2007). In: Peggy Chaudhry and Alan Zimmerman, *Protecting Your Intellectual Property Rights* (Springer New York 2013) 27.

it had identified over 10,000 accounts or users on *Facebook*, and 1,000 accounts on *Instagram* that sold counterfeits of its medicines.[1357]

The OECD has estimated the value of overall trade in counterfeit and pirated tangible goods at $250 billion in 2007, or 1.95% of worldwide trade.[1358] By 2016, this activity had grown to $509 billion, or 3.3% of global trade. For the EU, the value of counterfeit goods imports was estimated to have risen from EUR85 billion, or 5 % of total imports in 2013, to EUR121 billion (6.8% of total imports) in 2016.[1359] The social impact of these activities is manifold. Beyond the obvious economic loss to trademark owners and the dampening effect on innovation, this activity displaces legitimate employment, causes loss in public tax revenue and social security contributions, contributes to environmental pollution and may impact the health and safety of consumers.[1360]

Online marketplaces play an increasingly important role in the rise of counterfeit sales in general. They are even seen to be a key distribution channel.[1361] Fraudsters and innocent consumers alike use the characteristics of the internet, anonymity, flexibility and global reach for selling and

---

1357 OECD and European Union Intellectual Property Office, *Trade in Counterfeit Pharmaceutical Products* (OECD 2020) 48 <https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-pharmaceutical-products_a7c7e054-en> accessed 12 June 2020.

1358 'Magnitude of Counterfeiting and Piracy of Tangible Products – November 2009 Update' (OECD 2009) 1 <https://www.oecd.org/sti/ind/magnitudeofcounterfeitingandpiracyoftangibleproductsnovember2009update.htm> accessed 12 June 2020.

1359 OECD and European Union Intellectual Property Office, *Trade in Counterfeit and Pirated Goods: Value, Scope and Trends* (OECD 2019) 11–14 <https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en> accessed 12 June 2020. It should be noted that these results rely on customs seizure observations and do not include domestically produced and consumed counterfeit and pirated products; nor do they include pirated digital content on the Internet. The latter remains notoriously difficult to assess, although it can be assumed that a rising proportion of this trade is facilitated through online markets.

1360 'The Economic Impact of Counterfeiting and Piracy OECD - Executive Summary' (n 1355) 16–21; Frontier Economics (n 1133) 46–53. This report estimates that in 2013 between 2.0 and 2.6 million jobs and between $96 - 130 billion in tax revenue were lost due to counterfeiting worldwide. For the OECD region the loss in economic growth was valued between $30 - $54 billion in 2017.

1361 Europol and EU Intellectual Property Office, '2017 Situation Report on Counterfeiting and Piracy in the European Union' (2017) 53; Publications Office of the European Union, 'European Union Serious and Organised Crime Threat

buying counterfeit goods. The sheer market size and variety of offerings, the ability to deceive and attract customers with look-a-like sites and products, are additional reasons that have made online marketplaces a main target for counterfeiters.[1362] They are now joined by social media platforms, UGC sites and electronic messaging services that are either opening their own marketplaces or are being used to initiate transactions that are then conducted through other channels.[1363] Social media influencers are reported to unwittingly promote the sale of counterfeit items. The amount of active accounts identified as offering and selling counterfeits on sites such as *Instagram* is increasing constantly.[1364]

Counterfeiters have over the recent years infiltrated or bypassed traditional supply chains by using small consignments that enable shipments to customers directly from illicit warehouses or marketplaces in overseas locations. The proliferation of electronic payment services and electronic currencies, such as Bitcoin, has also helped this along. As more supply chain actors and intermediaries, from manufacturers, sellers and shippers to parcel delivery companies work digitally, the opportunities for fraud have moved to a new level.[1365] Although the Darknet is also being used for

---

Assessment : Crime in the Age of Technology.' (2017) Website 46 <https://publications.europa.eu/en/publication-detail/-/publication/a0c983b4-1db0-11e7-aeb3-01aa75ed71a1/language-en/format-PDF> accessed 17 August 2018. 'Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain' (n 223) 48–50.

1362 Chaudhry and Zimmerman (n 1355) 28. Roudaut, Mickaël R., 'From Sweatshops to Organized Crime: The New Face of Counterfeiting' in Christophe Geiger (ed), *Criminal enforcement of intellectual property: a handbook of contemporary research* (Edward Elgar 2012) 86–88. Jay Greene, 'How Amazon's Quest for More, Cheaper Products Has Resulted in a Flea Market of Fakes' *Washington Post* (14 November 2019) <https://www.washingtonpost.com/technology/2019/11/14/how-amazons-quest-more-cheaper-products-has-resulted-flea-market-fakes/> accessed 19 June 2020.

1363 Union (n 1360) 22–23. Andrea Stroppa and others, 'Instagram and Counterfeiting in 2019: New Features, Old Problems' (Ghost Data 2019) <https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf> accessed 20 October 2020.

1364 'How Social Media Behavior Influences Counterfeit Purchases' (*INCOPRO*, 25 February 2020) <https://www.incoproip.com/how-social-media-behavior-influences-counterfeit-purchases/> accessed 30 June 2020. In: 'Combating Trafficking in Counterfeit and Pirated Goods - Report to the President of the United States' (US Department of Homeland Security 2020) 22–23 <https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods> accessed 30 June 2020.

1365 Europol and EU Intellectual Property Office (n 1360) 53–54; EUIPO and Europol (n 1130) 37–39.

counterfeit sales, the legal or surface web remains the favoured channel as counterfeiters target the customer base of major consumer brands. Consumers, on the other hand, more often than not, are fully aware that they buy fake products. Research by the EU Intellectual Property Office (EUIPO) and the OECD has shown that almost 60% of consumers knowingly buy counterfeit products, a fact which doubtlessly helps sustain this activity. But the potential for deception is equally significant. Another study found that 39% of unwitting counterfeit purchases happen through online marketplaces, where it is more difficult for consumers to distinguish fakes from legitimate products.[1366] In any of these cases, the risk to people's health from buying counterfeits produced at substandard safety and quality is significant: unsafe electronic equipment, contaminated apparel, fake toys or jewellery containing dangerous substances, imitation car parts and counterfeit protective equipment are just some of the examples of products that can be found on online marketplaces and that can pose significant risks to consumers.

Meanwhile, the link between counterfeiting and organised crime, including the financing of terrorism, has become more and more publicised.[1367] In fact, online marketplaces are increasingly in the focus of law enforcement and regulators over the possibilities they open up to criminal activity and money laundering.[1368] Given the societal and economic impact, and the continued prevalence of this problem, trademark infringements conducted via online marketplaces have also moved into the focus the European Commission.[1369] The scale of the problem has even moved Amazon, the world's leading online marketplace operator, to spell this out in its 2018 and 2019 Annual Reports filed with the U.S. Securities and Exchange Commission. It stated that its policies and processes to prevent the

1366 'Combating Trafficking in Counterfeit and Pirated Goods - Report to the President of the United States' (n 1363) 15.

1367 UNIFAB, 'Counterfeiting & Terrorism, Edition 2016' (2015) <https://www.unifab.com/wp-content/uploads/2016/06/Rapport-A-Terrorisme-2015_GB_22.pdf> accessed 14 November 2019.

1368 Anton Moiseienko, 'Understanding Financial Crime Risks in E-Commerce' [2020] Royal United Services Institute for Defence and Security Studies 34.

1369 European Commission, 'Commission Staff Working Document Online Platforms Accompanying the Document Communication on Online Platforms and the Digital Single Market SWD(2016) 172 Final' (n 54) 21; European Commission, 'COM (2017) 555 Final' (n 69) 3, 7; European Commission, 'C(2018) 1177 Final' (n 8) Recitals 5, 10. European Commission, 'Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries - SWD(2019) 452 Final/2' (2020) 19.

sale of counterfeit, pirated and unlawful products by its sellers may be circumvented or operate insufficiently and that the company is at risk of being held liable for this.[1370]

Consequently, major online marketplaces have all been embroiled in high profile court cases brought by trademark owners. The prolific nature of many of these cases and their sheer number indicate the powerful economic interests involved.[1371] Deep pocketed global brand owners, mainly from luxury goods sectors, such as *L'Oréal*, *LVMH*, *Tiffany*, *Coty* or *PVH*, have sought to classify online marketplaces as direct infringers of their brands. Failing that, they sought to impose far reaching duties to prevent counterfeit sales. While at the beginning most of the defending platforms were small and more fragile players, many have now become major technology firms, horizontally and vertically integrated, often exceeding the size of their erstwhile opponents.

II. EU Trademark protection, its widening scope and the internet

Trademarks are one of the oldest intellectual property rights. The concept of trademark protection goes back to the time of the Industrial Revolution and the emergence of factory production. The increasing division of labour disconnected people from the production chain. It intensified competition through wider choice and fostered the circulation of goods and international trade.[1372] This also made it more difficult for producers and traders to distinguish their products from those of their competitors. Protection was sought against imitations and straightforward copying of products and brand names. Trademark law therefore originally aimed to a) indicate the origin of a branded good, and b) avoid confusion for the con-

1370 'Amazon 2018 Annual Report' (Amazon) 14 <https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx> accessed 19 June 2020; 'Amazon 2019 Annual Report' (Amazon) 14–15 <https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx> accessed 19 June 2020.

1371 See for example: *Tiffany (NJ) Inc. v. eBay Inc.* (n 599); *Google France v Louis Vuitton* (n 155); *L'Oréal v eBay* (n 463). *Coty v Amazon (FBA)* (n 590).

1372 WR Cornish, David Llewelyn and Tanya Frances Aplin, *Intellectual property: patents, copyright, trade marks and allied rights* (7. ed, Sweet & Maxwell [u.a] 2010) 640–642.

sumer, or any other ultimate user.[1373] Confusion may arise where a trademarked good is identical or similar to an already existing, earlier, or senior mark.[1374] The period after World War II saw the economic value of branded goods and trademarks rise exorbitantly, thanks to mass consumerism and globalisation, and aided by the sophistication of marketing and advertising. Brands have become commercially significant as intangible assets on companies' balance sheets. They are subject to substantive investments and even takeover battles.[1375]

Trademark law in the EU, similar to copyright, is founded on international agreements, notably the TRIPS Agreement and the 1883 Paris Convention for the Protection of Industrial Property.[1376] In the EU, a dual regime exists. Trademark owners may file for a Community Trademark which applies throughout the internal market and is enforced in a unitary way by the European Trademark Regulation (EUTMR).[1377] Alternatively, they may opt for national protection in one or several Member States of their choice, by registering their marks with national trademark offices, a right regulated under the EU Trademark Directive (EUTMD).[1378] The national trademark rights under the EU Trademark Directive are largely harmonised. Apart from the geographic scope, the substantial rights and protections and the conditions of use and revocation are largely the same as for the fully harmonised unitary EU Trademark (EUTM).[1379]

1373 *Hoffmann-La Roche & Co AG v Centrafarm Vertriebsgesellschaft Pharmazeutischer Erzeugnisse mbH, C-102/77* [1978] EU:C:1978:108 (CJEU) [7].

1374 The origin function, however, would only protect earlier registered marks against a later registration attempt of an identical mark, under Regulation (EU) 2017/1001 on the European Union trade mark 2017 (OJ L 154) Article 9 (2) (a), termed by Griffiths as "core zone" protection. Andrew Griffiths, 'The Trade Mark Monopoly: An Analysis of the Core Zone of Absolute Protection under Art. 5(1)(a)' [2007] Intellectual Property Quarterly 312, 314.

1375 Gordon V Smith, 'Brand Valuation: Too Long Neglected' (1990) 12 European Intellectual Property Review 159.

1376 TRIPS Articles 15-21; Paris Convention for the Protection of Industrial Property 1883.

1377 EUTMR.

1378 Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (Text with EEA relevance) 2015 (OJ L 336).

1379 ibid Recitals 5 & 8.Although it has been noted that some Member States, notably the UK, have made use of the option provided for in TRIPS Article 1.1 to afford a higher level of protection through their national laws, but this is only of limited relevance here. See for more detail: Althaf Marsoof, *Internet Intermediaries and Trade Mark Rights* (Routledge 2019) 47–50.

In line with the rise in commercial value of consumer brands, their owners have sought to expand the protection of trademarks beyond their essential functions. The arrival of the internet, notably e-commerce and online advertising, have only reinforced this trend.

Today, EU trademark law offers an "additional zone of protection"[1380] for well-known, or trademarks with a reputation,[1381] that goes beyond the core function of origin and the protection against confusion. The rationale behind this is, that reputed trademarks are at an additional risk of being taken unfair advantage of, or of being detrimentally affected by traders that use similar or identical marks for non-similar goods and services. This can be further broken down into acts that take unfair advantage of the distinctive character of a well-known mark (free-riding), are detrimental to the distinctive character of a well-known mark (dilution or blurring) and are to the detriment of the reputation of such a mark (tarnishment).[1382] This CJEU explored this in its *Interflora* ruling concerning trademark use in e-commerce. The UK retailer *Marks & Spencer's (M&S)* had purchased the search keyword "*Interflora*" and some variants on *Google's AdWords* referencing service. Customers typing these words into *Google's* search engines were led through sponsored links to *M&S's* own flower shop and delivery service. *Interflora* successfully complained that this use of its mark amounted to dilution and free-riding of its well-known mark, in addition to affecting the core function of origin protected under Article 5 (1) (a) of the previous version of the EUTMD.[1383]

The last 15 years have also seen a *de facto* extension of the unfair advantage protections for reputed marks to the core origin function of other than well-known marks. The CJEU did this by introducing the concept of the communicative functions of a trademark in *L'Oréal v Bellure*. The referring English court in this case had explicitly stated that the use of defendant *Bellure's* "smell-alike" perfumes did not lead to confusion with the consumer over the origin of its products. It wanted to establish, however, whether comparative advertising could still be considered as affecting the core and supplementary rights protected by trademark law. The CJEU

1380 Griffiths (n 1373) 314.

1381 EUTMR Article 9 (2) (c).

1382 *Interflora Inc, Interflora British Unit v Marks & Spencer plc, Flowers Direct Online Ltd, C-323/09* [2011] EU:C:2011:604 (CJEU) [73–95]; Ilanah Simon Fhima, 'Trademark Law and Advertising Keywords', *Research Handbook on EU Internet Law* (Edward Elgar 2014) 161.

1383 Directive 2008/95/EC to approximate the laws of the Member States relating to trade marks 2008. Equivalent to Article 9 (1) (a) of the EUTMR

took the view that a trademark owner also deserves protection for other than the core function of the trademark, namely that of guaranteeing the quality of the goods or services in question and those of communication, investment or advertising.[1384] This reasoning was then adopted by the CJEU in *Google France*,[1385] which confirmed the expanding scope of trademark protection. Keyword advertisers have since been more readily found to be primary liable for trademark infringements.[1386]

III. Enforcement: primary infringers or intermediaries with responsibilities?

a. Online intermediaries as primary infringers

The expanding protections afforded to trademarks, on the one hand, and the widening use of trademarks for advertising and marketing on e-commerce sites, on the other, are two trends that were bound to lead to legal conflict. While keyword purchasers[1387] and traders are more at risk of being seen as primary infringers, search engines or e-commerce marketplaces themselves have so far largely escaped liability for trademark infringements. Trademark law itself does not provide for remedies against contributory infringements. This means that intermediaries would need to meet the high bar of primary infringements if they were to be held liable under

---

1384 *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie v Bellure NV, Malaika Investments Ltd, trading as 'Honey pot cosmetic & Perfumery Sales', Starion International Ltd, C-487/07* [2009] EU:C:2009:378 (CJEU) [58]. The court referred to its deliberations in *Arsenal* and developed the Opinion of the AG in that case. *Arsenal Football Club plc v Matthew Reed, C-206/01* [2002] EU:C:2002:651 (CJEU) [51]; *Opinion of Advocate-General Ruiz-Jarabo Colomier, Arsenal Football Club plc v Matthew Reed, C-206/01* [2002] EU:C:2002:373 (CJEU) [46, 47].

1385 *Google France v Louis Vuitton* (n 155) para 102.

1386 Fhima (n 1381) 164.

1387 The CJEU confirmed in its rulings in *Google France* and *BergSpechte* that an advertiser who selects (search) keywords that are identical with a trademark in order to display advertising links that direct consumers to a website where its goods and services are offered, uses the sign in the course of trade. The advertiser can therefore be prevented by the trademark owner from using the disputed keywords: *Google France v Louis Vuitton* (n 155) paras 51, 52. *Die BergSpechte Outdoor Reisen und Alpinschule Edi Koblmüller GmbH v Günter Guni, trekking.at Reisen GmbH, C-278/08* [2010] CJEU EU:C:2010:163 [18].

trademark law. It is not that trademark owners have not tried to construe the activities of online intermediaries as directly affecting the protection of their marks, on the contrary. But in order to be found liable for confusing consumers over the origin of goods, affecting the communicative functions or taking unfair advantage of a reputed mark, a trader must first be making use of the sign in the course of trade.[1388] The concept of use is closer defined by a non-exhaustive list of actions, which includes for example the affixing of the sign to the goods, putting them on the market, importing and exporting, or using the signs in advertising.[1389] Since trademark law is a unitary right (where its concerns the EUTM), and significantly harmonised (where it concerns the national marks), any doubts over the interpretation of 'use' have ended up at CJEU level.

The three cases that deal with trademark infringement claims against online intermediaries (*Google France, L'Oréal v EBay* and *Coty v Amazon)* have so far all absolved these e-commerce marketplace and search engine operators from using the trademarks in the course of trade. In *L'Oréal v eBay*, defendant *eBay* was qualified as an infringer solely where it concerned its activity as a keyword purchaser for *Google AdWords*. Where it displayed trademarks in advertisings and online offers that belonged to third party sellers it was not found to use the trademark in a way that infringed the rights of the brand owners *L'Oréal*.[1390] In view of the vertically integrated nature of today's online platforms this concept can be challenged in itself, as will be seen from the *Coty v Amazon* ruling. The ruling in *L'Oréal v eBay* goes back to the *CJEU's* approach developed in *Google France*. French luxury group *LVMH,* and owner of the *Louis Vuitton* mark, brought infringement proceedings against *Google France.* The use of its trademark in the *AdWords* program, they claimed, had an adverse effect on the essential function of indicating origin and confused customers over the identity of its goods. Under the *AdWords,* program third parties could purchase the terms that made up its trademark in combination with other words, such 'imitation' or 'copy'. When users entered the keyword combinations into *Google's* search engine, sponsored links appeared on the results list, which led to offers that contained imitations of *Vuitton's* products. While the CJEU found that Google did indeed make use of the signs for which it

1388 EUTMR Article 9 (2).
1389 ibid Article 9 (3).
1390 *L'Oréal v eBay* (n 463) paras 89–95.

offered keyword search terms to third parties, it did not do this as part of its own commercial communications.[1391]

The commercial communications concept was a new element introduced into EU Trademark law, which the CJEU however failed to define more clearly, nor has this new requirement been identified by anyone else in more detail.[1392] It can be presumed that the CJEU wanted to express the fact that although *Google* used the signs for its own economic activity, that economic activity merely consisted of providing the technical facility for others to make use of the sign. That facilitation, however, had to be examined outside of the realms of EU trademark law.[1393] Consequently, the CJEU examined the role of *Google* under the ECD which led to the landmark ruling on the criteria of an active role of an intermediary referred to previously. Others have argued that *LVMH* may have had more success if it had asked whether *Google's* use took unfair advantage (free-riding) or happened to the detriment (dilution) of the distinctive character of its marks under the protection afforded to reputed marks. As it stands, search advertising platform operators' activities have so far not met the commercial communication requirement at the highest EU instance, and avoided being seen as engaging in infringing trademark use.[1394] The CJEU applied this methodology in *L'Oréal v EBay*, where it found that an e-commerce marketplace operator does not engage in infringing use of trademarks displayed on its site as part of product offerings and advertisements by its sellers.[1395]

In *Coty v Amazon*, perfume manufacturer *Coty (owner* of the *Davidoff* brand*)* brought an action against the American e-commerce giant's marketplace platform. *Coty* claimed that Amazon's activities were more than neutral due to its logistics service *Fulfillment by Amazon (FBA)*.This service allows sellers to not only sell through the platform's marketplace, but also have their products stored, shipped to customers, and, if needed, returned. *FBA* also offers other services to the seller, such as stock management and sales analytics. Not preventing and sanctioning the sales of counterfeits, *Coty* argued, made the marketplace directly liable for trademark violations. *Amazon* argued that its marketplace and logistics services had to be seen in separation, and that neither of the activities gave the company any active

1391 *Google France v Louis Vuitton* (n 155) para 56.
1392 Marsoof (n 1378) 37 fn 61.
1393 *Google France v Louis Vuitton* (n 155) 57.
1394 Marsoof (n 1378) 36–37.
1395 *L'Oréal v eBay* (n 463) para 102.

role in the intermediation process between sellers and buyers that amounted to use of the signs in the course of trade.

The referring *BGH* tentatively agreed with the previous instances,[1396] which had ruled that *Amazon's FBA* service was a merely neutral transportation and storage service that gave no rise to possession of the goods for the purposes of putting them on the market, i.e. causing a trademark infringement.[1397] However, the *BGH* still had doubts and asked the CJEU to clarify whether *FBA's* activity of storing goods on behalf of a third party constituted trademark use.[1398] First, the AG acknowledged in his Opinion the narrow reading of the *BGH*, which had evaluated the marketplace and the logistics operations of *Amazon* separately. As a mere storage facility that ignored the infringing nature of the stored goods, the marketplace operator would indeed not be liable. However, he also offered an alternative reading of the case. By examining the *FBA* activities in conjunction with the marketplace operations, he found that *Amazon's* vertically integrated service gave it a level of knowledge and control over the activities of its sellers that amounted to use of trademarks in the course of trade.[1399] *Amazon* engaged in an active and coordinated participation in the distribution of products, which not only amounted to a use of the trademark, but even gave it further duties to prevent infringements. It would be contrary to the economic realities of *Amazon's* business model to accept the company's fictitious separation of its activities into different (independent) distribution stages.[1400]

The CJEU, however, did not follow this assessment. Instead it underlined that it was obliged to stick closely to the referring court's questions, which had just asked for guidance on an intermediary that was stocking infringing goods without knowledge of such infringement.[1401] The admittedly unsatisfactory and reductionist qualification of the *BGH's* assessment of *Amazon's* role[1402] resulted in a rather sombre ruling in which the CJEU

1396 *Versand durch Amazon* [2016] OLG München 29 U 745/16, GRUR-Prax 2017 380.

1397 *Davidoff Hot Water III, I ZR 20/17* - [2018] BGH DE:BGH:2018:260718BIZR20.17.0, BeckRS 2018, 19562 [22].

1398 EUTMR Article 9 (3) (b).

1399 *AG Opinion, Coty v Amazon (FBA)* (n 591) para 51.

1400 ibid 59 fn 42.

1401 *Coty v Amazon (FBA)* (n 590) 20–24.

1402 Carina Gommers and Eva De Pauw, 'Liability for Trade Mark Infringement of Online Marketplaces in Europe: Are They "Caught in the Middle"?' (2020) 15 Journal of Intellectual Property Law & Practice 276, 285–286.

applied *Google France* by finding that a mere technical facility provider like *Amazon* did not engage in use of a trademark.[1403] The CJEU still left a backdoor open to the *BGH* by saying that *Amazon's* activities could only qualify as stocking for the purposes of offering or putting the goods on the market where it did itself pursue this aim. This was done in context of the fact that Amazon conceded during the proceedings that it could not clearly identify the original sellers of all of the branded products in question, which theoretically opened the possibility that some of these products were marketed on its own behalf.[1404]

This is in contrast to some recent, but still isolated, rulings at national level, where courts have been more assertive in finding vertically integrated Web 2.0 online marketplaces directly liable for trademark infringements. In the previously discussed UK case of *Cosmetic Warriors*,[1405] Amazon was found to be engaging in commercial communications of the *Lush* sign. Its internal search engine offered the term "*Lush*" to advertisers. The search results displayed a list of product offers by, a) third-party sellers using their own fulfilment services, b) third-part sellers using Amazon's FBA service and c) *Amazon* itself. However, none of the offers were *Lush* products. For the latter two categories *Amazon* clearly engaged in commercial communications to promote its own activities and was found liable.

In 2017, a French court found *Alibaba* guilty of counterfeiting acts according to the French intellectual property code.[1406] The company had offered on its website advertisements leading to counterfeit goods of the French outdoor brand *Lafuma*. The Paris court examined the integrated activities of the Chinese e-commerce giant, which consisted of, amongst others, special advertising services and account statuses offered to its sellers and the integration of payment and logistics services. This, in combination with an explicit intellectual property protection policy, gave the marketplace a level of control over the offers hosted for its sellers that conferred on it an active, editor role, that made use of the disputed sign in the course of trade. This was despite the fact that *Lafuma* was denied damages, because it could not prove financial losses due to this activity. Nevertheless, the court found *Alibaba* had also engaged in acts of unfair commercial practices, as the offers also deceived customers by selling counterfeit prod-

1403 *Coty v Amazon (FBA)* (n 590) para 43.
1404 ibid 48.
1405 *Cosmetic Warriors v Amazon* (n 560).
1406 *Lafuma Mobilier v Alibaba et autres* (n 580).

ucts.[1407] An indication of the criteria for the active role of marketplaces can also be gleaned from a 2017 ruling by France's Supreme Court.[1408] Although the claimant distributor was unsuccessful in its complaints against a selective distribution agreement, the court indicated *orbiter dictum* that the active role of an e-commerce marketplace like *Amazon* could be established from several factors: offering sellers to market their products internationally; payment services, notably cheque and bank card payments processing; product delivery, and solving problems that arise during order fulfilment.

Finally, in 2019 luxury shoe brand *Louboutin* successfully brought infringement claims against *Amazon* in Belgium.[1409] By examining the rulings of the CJEU, namely in *Daimler*,[1410] *Google France* and *L'Oréal v EBay* the Brussels Commercial Tribunal found that *Amazon* did use the *Louboutin* sign as part of its own commercial communications. The court did even go further than its UK counterpart in the *Cosmetic Warrior* case, which only found that *Amazon* used a sign as part of its commercial communication where it concerned *Amazon's* own offers (displayed as part of *Louboutin* keyword searches) and those of third-party sellers using *FBA*. The Belgian court ruled that *Amazon* also made use of the *Louboutin* sign where it displayed offers that were sold and fulfilled by third party sellers. By listing those offers and counting them towards "our selections" and "our fashion crushes" on its website, Amazon used the *Louboutin* sign to promote its own marketplace operations.[1411]

These judgements seem to indicate that the integrated and complex business models of current online marketplaces start to be seen legally for what they have been designed for commercially: controlling and monetis-

1407 The link between unfair commercial practices (UCPs) and sales of unlawful products under EU law will be explored in more detail in the next section. For a more detailed treatise of the link between UCPs and counterfeit sales under EU law see: Ansgar Ohly, 'Counterfeiting and Consumer Protection' in Christophe Geiger (ed), *Criminal enforcement of intellectual property: a handbook of contemporary research* (Edward Elgar 2012).

1408 *Concurrence v Amazon Services Europe, Samsung Electronics France* (n 585).

1409 *Christian Louboutin v Amazon Europe Core sarl* [2019] Chambre des actions en cessation du tribunal de l'entreprise francophone de Bruxelles A/19/ 00918. As discussed in : Nick Aries and Louise Vaziri, 'Online Intermediary Liability and TM Infringement: Stuck in the Middle With You' (2020) 9 Trade Marks 2020 A practical cross-border insight into trade mark work 1.

1410 *Daimler AG v Együd Garage Gépjárműjavító és Értékesítő Kft, C-179/15* [2016] CJEU EU:C:2016:134.

1411 Aries and Vaziri (n 1408).

ing to a maximum degree the content and interactions derived from users, be they customers, content creators, sellers, advertisers or others. If the sale of counterfeit products continues as it does on these data-driven super marketplaces, courts rightly appear to be readier in assigning primary liability. This tendency may be supported by the readiness of the EU legislator to assign primary copyright liability to large OCSSPs. It will be interesting to follow whether this trend materialises itself further and whether solid criteria for a primary liability approach will emerge. Meanwhile, less sophisticated platform models may only be subject to the various secondary liability avenues offered by EU and national laws. Search engines also appear to be out of scope for being found directly liable for trademark infringing use, except where it concerns the internal search functionalities of large online marketplaces.

b. Secondary liability trends and consumer law

With trademark law not providing direct legal tools for assessing the role of intermediaries, rightsholders will have to look to other enforcement tools offered by the law. As in other legal subject matter areas that relate to content, rightsholders in the area of trademarks have a wide arsenal of options at their disposal. This does not necessarily make for legal consistency, equality and efficacy across Member States when it comes to enforcing trademark rights and the fight against counterfeits. First, Articles 9 (1) (a) and 11 of IPRED give rightsholders the option to apply for injunctions against intermediaries. IPRED lays down general requirements of proportionality and efficacy for those injunctions, but leaves their execution to national laws. The result is similar to the findings detailed in the previous section on copyright: different national interpretations and legal traditions on the scope of these injunctions and the role and definition of intermediaries under IPRED vary. This makes for an inconsistent enforcement landscape across the EU.[1412] The ECD, the complimentary enforcement tool to the IPRED that sets the liability framework for online intermediaries, has also led to differing interpretations and inconsistent application. It shall suffice to note that, for example, the interplay between Article 11 IPRED

1412 European Commission, 'A Balanced IP Enforcement System Responding to Today's Societal Challenges, COM(2017) 707 Final' (European Commission 2017) 4; European Commission, 'Summary Response - IPR Enforcement' (n 173) 5, 15, 36–37.

and the liability conditions of the ECD in Articles 12 – 15 is not sufficiently clear, as can be seen from the unclarity over if and when injunctions imposed under IPRED would result in a violation of the general monitoring prohibition.[1413] Moreover different NTD requirements mean that some countries have imposed more detailed notification systems for IP related infringements on platforms and others have not.

Member States such as Germany have developed detailed and elaborate duty of care obligations for intermediaries from their jurisprudence in the area of trademark violations, which treat the question of the availability of the hosting defence as secondary.[1414] The UK has had more difficulties in adapting common law concepts to the area of secondary liability for trademark infringements, trying to explore concepts of accessory liability that are based on aiding or assisting in infringements.[1415] French jurisprudence on the availability and scope of secondary liability defences has been much more divergent. A recent comparison of the enforcement practices *vis-à-vis* intermediaries in Belgium, France, Germany and the UK testifies to the continuing heterogeneity in this area.[1416] The review noted the differences that existed in judicial practice when it came to defining the extent and nature of obligations of online hosts in terminating and preventing trademark infringements. This is despite the fact that trademark violations on online marketplaces have been an area of predilection at CJEU level for defining the reactive and preventive duties of search engines,[1417] online marketplaces[1418] and intermediaries in general.[1419]

1413 European Commission, 'Synopsis Report on the Regulatory Environment for Platforms' (n 539) 39.

1414 *Internetversteigerung I (Rolex v Ricardo.de), Az. I ZR 304/01* (n 567); *Internetversteigerung II (Rolex v Ricardo.de)* (n 568); *Internetversteigerung III (Rolex v Ricardo.de), Az. I ZR 73/05* (n 568); *Kinderhochstühle im Internet, I ZR 139/08* (n 722); *Kinderhochstühle im Internet II, I ZR 216/11* (n 584); *Kinderhochstühle im Internet III* (n 584).

1415 Marsoof (n 1378) 47–77.

1416 ibid 78–103.

1417 *Google France v Louis Vuitton* (n 155).

1418 *L'Oréal v eBay* (n 463).

1419 *Tommy Hilfiger Licensing LLC, Urban Trends Trading BV, Rado Uhren AG, Facton Kft, Lacoste SA, Burberry Ltd v Delta Center a.s, C-494/15* [2016] EU:C:2016:528 (CJEU); *Coöperatieve Vereniging SNB-REACT U.A. v Deepak Mehta - C-521/17* (n 276).

An additional enforcement dimension is introduced by the provisions of the Unfair Commercial Practices Directive (UCPD),[1420] which aims to protect consumers against traders that engage in misleading or aggressive marketing and sales practices. With e-commerce on the rise, the internet has also become an area were these unfair practices have been witnessed, be it through misrepresentation of goods, insufficient information or transparency about the products and services offered, or about the traders themselves.[1421] The sale of IP infringing goods, notably in the area of trademarks, would fall under such practices, where a trader confuses the consumer over the origins of a product.[1422] In that respect, both trademark and unfair competition rules go in the same direction. It has been unclear until recently, however, whether online marketplaces could qualify as traders under the UCPD. This would normally be assessed on a case-by-case basis.[1423] The new Omnibus Directive, passed in 2019, appears to solve this question in the affirmative by providing a definition of online marketplaces which would qualify them as traders both under the UCP and the Consumer Rights Directive.[1424] At the same time, this does not appear to deprive online marketplaces from the intermediary liability protections of the ECD. They can therefore be traders and ECD style information hosts at the same time. This creates a potential conflict between the rules of professional conduct imposed under the UCPD on traders hosting offers of unlawful products and the liability exemptions for these traders as online intermediaries.[1425] With regards to the sale of counterfeit goods, which can also be classified as an unfair commercial practice, the UCPD lacks any specific enforcement tools apt to deal with the role of marketplace traders that act solely as intermediaries. This remedy does however exist under IP legislation, namely through IPRED's Article 11. This exposes a gap in enforcement tools, which gives trademark rightsowners better protection

1420 Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market 2005 (OJ L 149).
1421 ibid Articles 5 - 9, and Annex I.
1422 ibid Article 6 (2) (a) & Recital 14. Ohly, 'Counterfeiting and Consumer Protection' (n 1406) 37–39.
1423 European Commission, 'UCP Directive Guidance' (n 57) 122–126. Valentina Moscon and Reto M Hilty, 'Digital Markets, Rules of Conduct and Liability of Online Intermediaries—Analysis of Two Case Studies: Unfair Commercial Practices and Trade Secrets Infringement' [2020] Max Planck Institute for Innovation and Competition Research Paper 27, 9–11.
1424 Omnibus Directive 2019/2161 (n 1249) Articles 3 & 4, Recital 25.
1425 Moscon and Hilty (n 1422) 13.

than consumers against the sale of IP infringing goods.[1426] Again, it should be kept in mind that the determination of liabilities and duties, and the enforcement mechanisms under these three regimes are to be settled by Member States according to their national interpretations and laws.

IV. Private enforcement

In response to global pressure from rightsowners, uncertainties in the application of intermediary legislation and a desire to bolster consumer trust, some online marketplaces started to implement more proactive voluntary mechanisms to prevent the occurrence of counterfeit products. NTD processes were the obvious, mandatory first line of defence. It should be noted here, that the detection and prevention of counterfeits and trademark infringing goods in general poses specific challenges that cannot easily be compared to fighting copyright infringements or unlawful speech. First, the sale of tangible goods, which is the most common area for trademark infringements on online platforms, is more difficult to analyse and intercept by a marketplace than it is for digital content.[1427] Often enough, product images and word filters have been the only elements available to an online marketplace operator to identify and assess potentially infringing products. A notice may give additional information and assurance from the side of the rightsholder. However, this is fraught with difficulties where the prevention of repeat infringements or voluntary proactive measures are concerned. Marketplaces would need to rely on specific brand and product knowledge and invest in investigative capabilities were they to effectively determine and fight counterfeits. Given the huge number of products and sellers on today's larger marketplaces this becomes an even greater challenge. The tools available to marketplaces have for a long time therefore been more basic than in the area of digital content recognition, relying more on ad-hoc, human verification. Once an infringing offer is removed, little stands in the way of the seller to offer the same products, which remains in its inventory, on other platforms, or through other distribution channels.[1428]

1426 ibid 15–16.

1427 Ullrich, 'Standards for Duty of Care?' (n 1137) 119–121.

1428 Content recognition technologies, such as watermarking or fingerprinting, are of limited use in this area.

Secondly, trademark law is complex and infringements are not restricted to counterfeiting. Counterfeits are usually double identity cases that are more straightforwardly illegal: the infringer imitates a trademark and the goods related to it. This is notwithstanding the fact that sophisticated counterfeits have become notoriously difficult to identify in some product areas.[1429] In light of the expanded protection afforded to trademark owners, determining infringing offers may become more complex, for example, where it concerns issues of free-riding, tarnishment or blurring of reputed marks. The international and even global nature of many online marketplaces also opens the door to grey market sales, parallel imports or violations of selective distribution agreements.[1430] Added to this are various other problems, for example with sales of generic replacement or accessory parts for OEM products, such as printer cartridges, mobile phone chargers or cables etc. Many of these problems can overlap with other legal problems, such as product compliance, product safety or unfair commercial practices, like misrepresentation.[1431] The latter borderline issues are far from easy to determine, even for rightsowners. Not in every case do they necessarily restrict the rights of a brand owner. In effect, they may even be subject to abusive notices, aimed at removing legitimate competitors.[1432]

The flood of NTDs that accompanied the rise of online marketplaces has been processed largely manually until recently. The amount of counterfeit notices that online marketplaces receive from rightsowners is however difficult to establish. Unlike in the areas of hate speech or copyright, the leading online marketplaces remain remarkably nontransparent about their NTD practices. Of the pure online marketplaces, only *Etsy*, a significantly smaller competitor to *Amazon*, *Alibaba*, *eBay* or *JD.com*, has published a transparency report, albeit only until 2016. According to the report, it received 18,857 notices, which resulted in the removal of 235,201 listings from 59,131 sellers. Altogether, the company saw an increase in IP related takedowns by 70% compared to the previous year. Measured by seller gross merchandise value (GMV, the total value of goods sold), the company was about 20 times smaller than *Amazon's* marketplace and 18 times smaller

1429 EUIPO and Europol (n 1130) 8–19.

1430 *Coty Germany GmbH v Parfümerie Akzente GmbH, C-230/16* [2017] CJEU EU:C:2017:941.

1431 Robert W Payne, 'Unauthorized Online Dealers of "Genuine" Products in the Amazon Marketplace and beyond: Remedies for Brand Owners' [2014] J Internet Law 3.

1432 Greene (n 1361).

than eBay in 2016.[1433] Other detailed counterfeit or trademark removal data is only available from the Transparency Report of *Facebook*.[1434]

The complexity of assessing trademark infringements and managing NTD requests together with the looming threat of legal conflict with brand owners was accompanied by emerging diligent economic operator responsibilities principles through case law.[1435] This created strong incentives to operationalise and pre-empt the sale of counterfeits and trademark infringements by using technology and by fostering cooperation with rightsowners. Online marketplaces initially launched programs that gave brand owners specific means to identify, flag and have listings removed. *EBay* was the pioneer in this regard with its *Verified Rightsowner Program* (*VeRo*), launched in 1998. This program had 31,000 rightsowner members in 2014. In 2008, the company removed 2.1 million listings through this program and another 2 million proactively.[1436] Both *Amazon* and *Alibaba* have also started similar programs, albeit almost more than 15 years after *eBay*.[1437] This happened often after serious pressure from brand owners. However, here again, the mechanisms and takedown modalities, including counterclaims, remain opaque and generally inaccessible to outsiders. These programs appear to forge deeper relationships, mainly with large brand owners. The latter will be able to liaise directly by exchanging product and brand information with the internal teams at these platforms that are responsible for identifying and taking down allegedly infringing offers. At *Amazon*, these special relationships have gone even further. In 2016 the company started to "gate" certain brands on its sites.[1438] This means brand

1433 According to the following resources: 'Research' (*Marketplace Pulse*) <https://www.marketplacepulse.com/research> accessed 19 June 2020; 'Etsy Annual GMV 2019' (*Statista*) <https://www.statista.com/statistics/219412/etsys-total-merchandise-sales-per-year/> accessed 19 June 2020.

1434 Facebook, 'Intellectual Property' <https://transparency.facebook.com/intellectual-property/jan-jun-2017> accessed 5 June 2020.

1435 E.g. in *L'Oréal v eBay* (n 463). And national case law mentioned Chapter 3

1436 'EBay Drives Commitment to Fight Counterfeiting and Piracy' (28 October 2014) <https://www.eBayinc.com/stories/press-room/uk/eBay-drives-commitment-to-fight-counterfeiting-and-piracy/> accessed 19 June 2020.

1437 'Amazon Brand Registry: Help Protect Your Brand on Amazon' <https://brandservices.amazon.com/> accessed 19 June 2020; 'Alibaba Group - Intellectual Property Protection Platform (IPP Platform)' < https:////ipp.alibabagroup.com/index.htm> accessed 19 June 2020.

1438 Gordon Mcconnell, 'Amazon Starts "Brand Gating" to Stop Counterfeits' (1 September 2016) <https://blog.redpoints.com/en/amazon-plans-to-combat-counterfeits> accessed 19 June 2020.

owners may restrict the sale of their brands on the *Amazon* marketplace either to themselves or to a select number of sellers. Those sellers would either be pre-authorised by the brand owner and/or they would need to provide a proof of authenticity for the products they intend to sell. This happens mainly were large manufactures have opened customised brand shops on the *Amazon* website.[1439] On the one hand, it makes sense to engage brand owners more proactively in the fight against counterfeit products. On the other hand, this privileged relationship is relatively obscure and may lead to a predominance of already large and established brands on these marketplaces, potentially imposing a disproportionally high burden of proof on smaller sellers.[1440]

Apart from these relationship programs, many online marketplaces have been ramping up their automated counterfeit identification technologies. As stated above, *eBay* has worked on proactive removals as early as 2008. French online marketplace *PriceMinister* has been using automated software to detect counterfeits, supported by manual checks, since 2006.[1441] *Etsy* also confirms the use of automated tools in conjunction with community flagging and manual investigations to protect the integrity of its marketplace. Meanwhile the two dominating players, *Alibaba* and *Amazon*, use their brand owner relationship programs, *Brand Registry (Amazon)* and the *IP Protection Platform (Alibaba)*[1442] to fast-track the development of proactive, automated identification tools for rightsowners. The idea here is that interaction and information exchange with brand owners will help to improve automated tools developed to proactively identify and remove suspected counterfeit listings. In the case of *Alibaba*, this includes "image recognition algorithms, including optical character recognition (OCR) technology, product intelligence learning algorithms, a product information library, counterfeit screening models, semantic recognition algorithms, and a real-time interception system."[1443]

1439 See for example: 'Olay' (*Amazon.co.uk*) <https://www.amazon.co.uk/stores/Olay/Olay/page/3BBAE664-6ADE-4D62-86AD-A052F323E900> accessed 19 June 2020.

1440 Mcconnell (n 1437).

1441 *L'Oreal SA v. eBay International AG* (n 563) paras 267–276.

1442 'Alibaba's Enhanced IP Protection Platform Now Eliminates Fake Listings in Less than 24 Hours' (10 August 2017) <https://alibabagroup.com/en/news/article?news=p170810> accessed 19 June 2020. 'Amazon Brand Gating Increases Merchant Suspension Risk' (*TameBay*, 22 February 2019).

1443 'AACA Practices' (*Alibaba Anti-counterfeiting Alliance*) <https://aaca.alibabagroup.heymeo.net/> accessed 25 June 2020.

Amazon took this a step further in 2019 with its *Project Zero*, by allowing selected brand owners of their *Brand Registry* program to remove listings through "self-service counterfeit removals". This information will feed into its proactive tools that already scan the five billion listings updates that are registered every day on its platform, presumable by using a similar array of methods and technologies as *Alibaba*.[1444] The company stated that in 2018 it had spent $400 million, and in 2019 $500 million on efforts to combat fraud, which includes counterfeiting on its platform. It employed 8,000 people in the fraud detection space and blocked 6 billion fraudulent listings and 2.5 million "bad actors."[1445]

There is no self-organised industry initiative, as for example the GIFTC in the area of terrorist content, where online marketplaces join forces on a technical level and exchange best practices. On the other hand, industry associations such as the *International Chamber of Commerce (ICC)*, which represent the interests of many of the large trademark owners have been more proactive. The ICC's initiative *Business Action to Stop Counterfeiting and Piracy (BASCAP)*, has, for example, issued more detailed guidance, setting out best practices and concrete measures that platforms should take in the fight against trademark infringements.[1446] These suggestions, although purely voluntary, could provide useful reference points in formulating enhanced legal responsibilities for online marketplaces. An example for such a duty of care standard for e-commerce platforms, developed as part of the research for this work, is presented in Chapter 6 and ANNEX III.

Online marketplaces appear to be individually developing and employing their prevention systems and technologies, based on the proprietary transaction and user data and the brand intelligence harvested through

---

1444 'Amazon Project Zero: Empowering Brands against Counterfeits' <https://brandservices.amazon.com/projectzero> accessed 25 June 2020; Stephanie Condon, 'Amazon's Project Zero Lets Brands Take down Counterfeits' (*ZDNet*, 28 February 2019) <https://www.zdnet.com/article/amazons-project-zero-lets-brands-take-down-counterfeits/> accessed 25 June 2020.

1445 Kiri Masters, 'The One Change That Would Drastically Reduce Counterfeiting On Amazon's U.S. Marketplace' (*Forbes*) <https://www.forbes.com/sites/kirimasters/2019/11/13/the-one-change-that-would-drastically-reduce-counterfeiting-on-amazons-us-marketplace/> accessed 25 June 2020; 'Amazon Ramping Up Efforts To Take Down Counterfeiters' <https://finance.yahoo.com/news/amazon-ramping-efforts-down-counterfeiters-173702229.html> accessed 25 June 2020.

1446 'Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain' (n 223); BASCAP, 'Best-Practices-for-Removing-Fakes-from-Online-Platforms' (BASCAP 2016).

their systems. Like in other areas, law enforcement and authorities have had difficulties in establishing working contacts and information exchanges with these marketplaces. The preferred practice has been to suspend or ban offending actors (sellers, consumers, advertisers) from their sites and close the case. This practice seems to be under review, however. *Alibaba* and *Amazon* have recently indicated that they intend to work more closely with authorities and law enforcement in this area.[1447]

Both, larger and smaller e-commerce platforms may already have extensive seller data, including VAT numbers, payment details, business addresses, detailed sales and product records, which may even include manufacturer data, or customer data on shopping behaviour and shipping addresses.[1448] The number of other intermediaries that vertically integrate their services into online marketplaces is usually higher than in other areas. Payment services, logistics providers, advertisers may also provide additional data and leverage. Compared to other areas of online interactions – e.g. speech and digital content sharing – users in e-commerce are also more deeply integrated with the platform. Sellers need to provide product data and banking details, and consumers may need to provide verified credit card and address details. This, combined with existing transparency and due diligence obligations under other statutes, for example for food sellers,[1449] online pharmacies[1450] or anti-money-laundering laws,[1451] make for a powerful amalgam of intelligence. The increasingly vertically and horizontally integrated online marketplaces and other platforms have therefore ample data on which sophisticated automated infringement prevention tools, based on predictive analysis, can be built. These would usually be in-

1447 Rich and Ho (n 602) 10–11; Todd Bishop, 'Amazon Forms "Counterfeit Crimes Unit," under Pressure to Escalate Fight against Fake Products' (*GeekWire*, 24 June 2020) <https://www.geekwire.com/2020/amazon-forms-counterfeit-crimes-unit-pressure-escalate-fight-fake-products/> accessed 25 June 2020.

1448 Nizan Geslevich Packin and Yafit Lev-Aretz, 'Big Data and Social Netbanks: Are You Ready to Replace Your Bank?' (2016) 53 Houston Law Review 1211, 1223–1242.

1449 Regulation (EC) 852/2004 of 29 April 2004 on the hygiene of foodstuffs 2004 (OJ L 139) Article 6 (2).

1450 Directive 2011/62/EU of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products 2011 (OJ L 174, 172011) Article 85 c.

1451 Directive 2015/849/EU of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 2015 (OJ L 141, 562015) Articles 13, 14, Recital 18.

tegrated into wider (online) fraud detection programs. Larger platforms may, however, be in a privileged position to develop and deploy effective anti-counterfeiting technologies due to their superior data collection activities, financial power and special relationship with large brand owners.

Amazon, for example has started to develop its own fraud detection product, based on machine learning, to predict and spot fraudulent online activities. The service is offered to any e-commerce business and is run from its own *AWS* cloud system.[1452] It is understandable that fraud detection mechanisms cannot be disclosed liberally for public scrutiny. Nevertheless, as of now the mechanisms, and broader criteria and outcomes of the blocking, removal and seller sanction processes are secretive and inaccessible. This would need to be considered when solutions for any enhanced duties of care obligation that rely on state-of-the-art prevention tools are being designed.[1453] First, it would be essential that competing (smaller) platforms have access to an array of market solutions that are not dominated by proprietary systems of the current incumbents. Secondly, transparency obligations would need to be established that allow at least for scrutiny on the side of regulators and public authorities, in order to address risks relating to data protection, privacy, competition, consumer protection and freedom of expression.

V. EU policy development

Despite the prominence that the fight against counterfeits and the protection of IP rights via the internet has received, EU policy action has remained relatively subdued in this particular area. As stated, intermediary liability cases concerning trademark infringements have been a common feature since the early days of the ECD.[1454] The European Commission acknowledged in its 10-year review of the ECD that counterfeit sales continued to be a problem for the development of e-commerce and the Single

1452 'Amazon Fraud Detector - Amazon Web Services' (*Amazon Web Services, Inc.*) <https://aws.amazon.com/fraud-detector/> accessed 25 June 2020.

1453 DSM Directive 2019/790 Article 17 (4 b); European Commission, 'Impact Assessment 3/3 - DSM Directive' (n 1306) 167–172. The DSM Directive, for example, prescribes the use of industry standard prevention methods in the area of copyright and was accompanied by a market review of available content recognition tools outside *Google's Content ID* product.

1454 Verbiest and others (n 644) 36–38, 91–93.

Market.[1455] It announced that, apart from promoting self-regulatory initiatives in this area, it would address the problem through a review of IPRED[1456] under its Intellectual Property Strategy.[1457] The persistence of the problem was confirmed in 2016 in the Commission's DSM communication.[1458] The European Commission's strategy paper on online platforms and the DSM of 2016, however, put the focus of legislative action on copyright and the fight against harmful content on VSPs under the AVMSD.[1459] Trademark infringements and intermediary liability also occupied a less prominent space in both the 2017 Communication and the 2018 Recommendations on tackling illegal content online. These documents focussed more prominently on the area of copyright, hate speech and terrorist content. Meanwhile, the IPRED review resulted in a Guidance document that sought to clarify, amongst others, the scope of injunctions available against intermediaries. Voluntary agreements between stakeholders are at this stage the only tangible policy action at EU level.

a. Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet

The 2011 Memorandum of Understanding (MoU), initiated by the Commission, brought major rightsholders, trade associations and online marketplaces to the table.[1460] The aim of the MoU was to achieve closer cooperation and develop a consensus on standards and measures relating to: NTD systems, the exchange of information regarding infringements, proactive measures, dealing with repeat infringers and cooperation with law enforcement and customs authorities. The MoU also committed to the development of key performance indicators (KPIs) to measure implemen-

1455 European Commission, 'SEC(2011) 1641 Final' (n 11) 72.
1456 ibid 74. European Commission, 'E-Commerce Action Plan 2012-2015, State of Play 2013, SWD(2013) 153 Final' (n 537) 18–19.
1457 European Commission, 'A Single Market for Intellectual Property Rights - Boosting Creativity and Innovation to Provide Economic Growth, High Quality Jobs and First Class Products and Services in Europe, COM(2011) 287 Final' (2011).
1458 European Commission, 'Commission Staff Working Document Online Platforms Accompanying the Document Communication on Online Platforms and the Digital Single Market SWD(2016) 172 Final' (n 54) 21.
1459 European Commission, 'COM(2016) 288 Final' (n 223) 8–9.
1460 'Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet, 2011' (n 665).

tation of the agreed commitments.[1461] The commitments are, however, relatively loose, abstract and do not more than reflect the status quo of operational procedures and legal requirements of the ECD. For example, marketplaces commit to efficient and swift reactions to NTD requests, the implementation of commercially reasonable and available proactive and preventive measures, or to implementing repeat infringer policies. Swift reactions to notifications are already required by Article 14 (1) ECD. Secondly, all the three platforms which signed the MoU initially were engaged in some way in proactive measures to detect trademark infringing goods, although the degree of this activity remained largely unknown. The MoU does not provide any additional clarification or commitment in this matter. Finally, the need to act against repeat infringers had been voiced by the CJEU's AG in its Opinion in the *L'Oréal v eBay* case,[1462] which was later confirmed in the CJEU's ruling.[1463] The agreement can be seen as an important, but rather symbolic step,[1464] aimed principally at getting the various stakeholder talk to each other. The progress report on the MoU[1465] two years later showed mixed success. The tenor of the report implies that information sharing, the agreement on KPIs and the transparency on proactive measures by platforms were problematic areas. On the positive side, it appears to have strengthened at least bilateral links between stakeholders, leading to more efficient counterfeit identification and removal processes in specific situations.

The MoU was renewed in 2016,[1466] albeit without making any changes to the 2011 text, except for some new, high level KPIs. These rather basic performance metrics, which were inherently difficult to reach agreement on, as can be seen from the five years it took to agree to them, are: the

---

1461 ibid. Apart from major consumer brands the MoU was also signed by *Amazon*, *eBay* and *Rakuten (PriceMinister)*

1462 *Opinion of Advocate General Jääskinen, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd and others, C-324/09* [2010] EU:C:2010:757 (CJEU) [168, 182].

1463 *L'Oréal v eBay* (n 463) 141.

1464 L Smith, 'European Commission Publishes Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet' (2011) 6 Journal of Intellectual Property Law & Practice 770.

1465 European Commission, 'Report on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet /COM/ 2013/0209 Final' (2013) COM/2013/0209 final <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013DC0209> accessed 17 March 2017.

1466 'Memorandum of Understanding on the Online Sale of Counterfeit Goods, 2016' (n 542).

number of search results that lead to counterfeit listings;[1467] the number of listings removed following proactive measures by platforms and rightsowner NTD requests; the number of restrictions imposed on sellers. The 2017 report on the functioning of the MoU attests to the ongoing problems of counterfeit sales via marketplaces. According to the first KPI, brand owners that searched marketplace platforms between May to June 2017 reported that on aggregate 14.3% of the top 100 listings of their searches were counterfeits. The report also notes that 97.4% of removals on the participating online marketplaces were made through proactive and preventive systems, which were, however, prone to false positives.[1468] Despite the success of closer and better cooperation on NTD procedures and information exchange, there remained room for improvement. A lack of transparency in how KPIs are collected by platforms remained an issue, according to the report, as did more detailed information on NTD and proactive procedures applied by platforms.

The report concluded that common standards on repeat infringer sanctions and content removals would further improve efficiencies in identifying infringers on the side of rightsowners.[1469] The 2020, more detailed Report on the Functioning of the MoU, seems to indicate that the problems reported in 2017 have not gone away.[1470] The Commission notes that the reporting of the KPIs is of limited value due to methodological inconsistencies in data collection and disagreements between signatories about the interpretation of the numbers obtained from these exercises.[1471] The first KPI (% of search results leading to counterfeit offers) is not reported any longer. Instead, just an indication is given about the oscillating trend in this KPI over the last three years.[1472] The number of listings removed following proactive measures by platforms remained high and varied between 90% and 98% during the six data collection exercises since 2017. Da-

1467 In % of the top 100 listings in a certain product category of a certain brand.

1468 European Commission, 'Overview of the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet, SWD(2017) 430 Final' (European Commission 2017) 7. Alibaba and Allegro had also joined the MoU by 2017.

1469 ibid 11–13.

1470 European Commission, 'Report on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet, SWD(2020) 166 Final/2' (2020) SWD(2020) 166 final/2 <https://ec.europa.eu/docsroom/documents/42701> accessed 27 August 2020.

1471 ibid 7, 11–13.

1472 ibid 8–9.

ta on the third KPI, the number of restrictions imposed on sellers, also remained inconclusive, due to only half of the participating platforms providing feedback on this indicator and one platform not providing data on repeat infringer sanctions.[1473] The feedback on the KPI collection process appears to demonstrate a continuing rift between online platforms and rightsowners over methodologies, readiness to report, the interpretation of the numbers and how to address efficiency gaps in the working of the MoU. On the positive side, the recurring meetings seem to have strengthened relationships between rightsholders and platforms and have led to some bilateral cooperation. Most platforms that participate in the MoU use automated and proactive systems for identifying and removing counterfeit goods. While decision accuracy and false positives remain problems, rightsowners and platforms work increasingly together to define criteria that help platforms in risk profiling for the application of automated tools. However, platforms note that these measures are resource-intensive and would need to remain proportionate and reasonable.[1474] Meanwhile, the use of brand protection programs by platforms is on the rise.[1475] It is endorsed by and large by platforms and rightsowners as an effective means to identify counterfeits.

There remain, however, significant differences about the state of repeat infringer enforcement measures. Rightsholder denied that any significant progress has been made in this matter, thus throwing doubts on the seller vetting and onboarding processes of platforms. Online platforms, however, insisted on the need to remain flexible in the application of these policies.[1476] The European Commission and rightsholders see the recent Platform-to Business Regulation (P2B) as a useful tool for bringing more transparency into operational practices of online platforms, especially where it concerns setting out and implementing sanctioning policies for repeat infringers.[1477] Rightsholders also called up the recent Market Surveillance Regulation 2019/1020 (MSR) in the area of product regulation, which im-

1473 ibid 9–10.
1474 ibid 20–21.
1475 ibid 22.
1476 ibid 27–30.
1477 Platform-to-business (P2B) Regulation 2019/1150 (n 1248) Articles 3 & 4; European Commission, 'MoU Progress Report - SWD(2020) 166 Final/2' (n 1469) 23, 26. Articles 3 and 4 requires that online intermediation services, which includes search engines and e-commerce marketplaces, have clear terms and conditions in place, as well as transparent sanction processes for repeatedly infringing business users.

poses an obligation on ISSPs to cooperate with authorities in the fight against products that pose compliance and safety risks.[1478] Meanwhile, three rightsholders from the luxury sector withdrew from the MoU in January 2020 due to insufficient progress. In 2019, *Facebook (Marketplace)* joined the MoU bringing the total number of participating online platforms to six.

Looking at the technological progress in proactive measures, expedited NTD procedures and private information sharing over the last 10 years, it is surprising that the 2016 MoU is based on the exact loose and basic criteria as its previous version of 2011. There would have been a chance to commit to more ambitious principles and standards both on the side of platforms and rightsholders, but this was expressly rejected in the last 2020 progress report.[1479] Despite the creation of doubtlessly useful KPIs, there is no further evidence of common standards emerging in the fight against trademark infringements committed via online intermediaries. Arguably, the best practices shared in the 2020 Report are too little considering that the MoU goes into its tenth year of existence.

Transparency on the enforcement procedures remains a major problem not only where it concerns relations with the owners of the trademark rights, but also where cooperation with authorities is concerned. With the intricacy and complexity of trademark law and the rise of automated takedowns, there is a clear need to protect against the risk of abusive notices and faulty decisions in the many possible borderline cases.[1480] Platforms' self-styled enforcement mechanisms may have a significant effect on sellers and consumers. The current situation of private agreements between platforms and rightsholders, and the rise in automated tools, may eventually have an anti-competitive effect and restrict consumer choice. There is a real risk that these private ordering style arrangements benefit only the economically powerful stakeholders and preclude the dynamic adaption of

1478 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance.) 2019 (OJ L 169) Article 7 (2); European Commission, 'MoU Progress Report - SWD(2020) 166 Final/2' (n 1469) 34.

1479 European Commission, 'MoU Progress Report - SWD(2020) 166 Final/2' (n 1469) 38.

1480 Marsoof (n 1378) 150, 168; Frederick W Mostert and Martin B Schwimmer, 'Notice and Takedown for Trademarks 100th Anniversary Issue' (2011) 101 The Trademark Reporter 249, 278–279.

the responsibilities of intermediaries.[1481] However, despite of the persisting problem of counterfeit sales through online marketplaces and the opacity of the rapidly evolving private enforcement processes, there appears to be no intention of further policy action on the side of the European Commission. Yet, public scrutiny is needed more than ever.[1482]

b. Other EU policy initiatives

Compared to digital content and copyright, the policymaker has more alternatives when it comes to disrupting the supply chain of counterfeit products. To that effect, the European Commission has been more active in neighbouring policy areas. It strengthened, for example, the enforcement powers of EU customs authorities relating to the seizure and prosecution of IPR infringements.[1483] In addition, the "follow the money" approach aims to limit the means of fraudsters and other economic actors to profit from the sales of infringing goods via the internet. In 2018, the European Commission brought advertising intermediaries into the game by forging an MoU by which these actors commit to avoiding the placement of adverts on websites that sell and share counterfeit and copyright infringing goods and content.[1484] Anti-money laundering obligations imposed on online platforms, which integrate payment services into their operations, would provide an additional way to freeze assets of counterfeiters and pursue them criminally. Currently, authorities are only starting to look at this enforcement channel.[1485] Most of the larger online platforms own financial service entities that are regulated by EU Member States' financial supervision authorities.[1486] Other intermediaries that interact with online platforms are transportation or logistics service providers, or payment in-

1481 Dinwoodie (n 312) 471.
1482 ibid.
1483 Regulation (EU) No 608/2013 concerning customs enforcement of intellectual property rights 2013 (OJ L 181).
1484 European Commission, 'Memorandum of Understanding on Online Advertising and Intellectual Property Rights' (n 542).
1485 Moiseienko (n 1367) 14.
1486 The following online platforms have subsidiaries that are registered and regulated as financial services in the EU: *Google* – as electronic money institution (EME) and payment institution (PI) in Lithuania and Ireland, respectively; *Facebook* – as PI and EME in Ireland; *Microsoft* – as PI in Ireland; *Amazon* and *AliExpress* - as EMEs in Luxembourg; *eBay* and *AirBnb* - as PIs in Luxembourg; *Rakuten* - as a bank in Luxembourg; *Uber* – as an EME in the Netherlands;

termediaries.[1487] Apart from the concrete responsibilities of platforms discussed above, diligently operating (multi-sided) marketplaces should be aware of the opportunities and threats that these various supply chain intermediaries present in the fight against unlawful products and content.

Lastly, the draft DSA now appears to partly address the enforcement gaps with regards to trademark infringements on online marketplaces through the imposition of traceability requirements and onboarding due diligence requirements for traders.[1488] These know-your-customer (KYC) style obligations had been demanded by brand owners and other commentators for some time as a means to force due diligence on platform operators in the fight against counterfeits and non-compliant products.[1489]

VI. Summary and outlook

The sale of counterfeits and other trademark infringing products via online platforms has been a significant problem, causing economic damage to rightsholders and important risks to consumer trust and safety. While trademark law provides unitary protection in the EU against primary infringers, secondary liabilities are outside of its scope. The enforcement of the latter has, however, often been frustrated by the disparate national interpretations and applications of the remedies provided by IPRED against intermediaries. Meanwhile, the intermediary liability provisions of the ECD have met the same unsatisfactory patchwork applications as in many other content areas. CJEU guidance on the duties and liabilities of Web 2.0. online marketplaces and search engines have not brought the clarification sought, although they created cornerstone responsibility concepts, such as the diligent economic operator.[1490]

---

searches conducted in the Public Supervision Register of *De Nederlandsche Bank* on 27.08.2020: 'Public Register - De Nederlandsche Bank'

1487 J Bruce Richardson, 'With Great Power Comes Little Responsibility: The Role of Online Payment Service Providers with Regards to Websites Selling Counterfeit Goods' (2014) 12 Canadian Journal of Law and Technology <https://ojs.library.dal.ca/CJLT/article/view/6607> accessed 20 March 2017.

1488 European Commission DSA proposal (n 10) Article 22, Recital 49.

1489 European Commission, 'Summary Response - IPR Enforcement' (n 173) 17, 44; Ullrich, 'Standards for Duty of Care?' (n 1137) 125; Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 243–245.

1490 *L'Oréal v eBay* (n 463) paras 120–124.

In the by now familiar battle to seize primary infringers on the internet, online marketplaces as middlemen have moved into the focus of rightsowners when it comes to the enforcement of their economic rights. Rightsowners have sought relief by imposing primary liabilities on the likes of *Google Search*, *EBay* and *Amazon*. These efforts, too, have until recently been fruitless. Courts refused to attribute to online marketplaces and search engines any part in the use of trademarks in the course of trade. In some Member States, however, things appear to be changing. This has certainly been aided by the constant expansion of trademark protection during a time of globalisation and consumer focus on brands. But it is also a signal that the manifold ancillary services of integrated online platforms, such as advertising, search, payment services, order fulfilment, complaints handling, sales and fraud analytics, or even fincial services,[1491] make these intermediaries appear in a changing light: they actively and selectively promote third party commerce and derive data and financial benefits from the commercial services they provide to sellers and consumers.

In the shadow of this dispersed and unclear legal picture, online marketplaces have started to build their own private enforcement processes. First, obligatory NTD processes have been enriched with expedited and customised removal processes granted to economically powerful rightsholders. Secondly, rightsholders are hauled into the enforcement efforts of platforms by being involved in the authorisation and removal of products sold by sellers or by providing brand-specific intelligence. Third, most online marketplaces have been developing their own automated prevention tools for spotting and removing trademark infringing goods. These processes are, however, buried in obscurity. Consequently, it is not clear how the risk of abusive notices and potential anti-competitive behaviour by major brands is being contained.

Policy action on the side of the EU lawmaker has been limited to self-regulatory codes of practice. Two successive MoUs produced high level KPIs, that, once implemented, testified to the ongoing problem of counterfeit sales and the rise of automated enforcement systems by platforms. Apart from better cooperation between rightsholders and platforms, and anecdotal evidence of better enforcement against infringers, the Commission repeatedly noted a clear need for further improvement over the almost 10 years of existence of the MoU. The self-regulatory efforts have so far not brought the transparency sought by rightsholders over the manda-

1491 'Amazon Lending' <https://sell.amazon.com/programs/amazon-lending.html> accessed 29 June 2020.

tory NTD processes and proactive measures. More importantly, this transparency is also amiss for sellers and consumers. The P2B Regulation[1492] and the Omnibus Directive[1493] will help improve transparency to business users and consumers on the underlying ranking and display mechanisms of internal search results. They will also raise due diligence standards of platforms to some extent, by obliging them to ensure sellers clearly state whether they act as professional traders or private individuals.[1494] This obligation has been carried over into the DSA proposal as a condition for an exemption from consumer law liabilities.[1495] However, clearer positive obligations for platforms when it comes to creating an environment that discourages the sale of counterfeit products are still wanting. The traceability due diligence obligations proposed by the new DSA may be a useful first step in this direction.[1496]

Meanwhile, the US Government completed its more comprehensive review of intermediary liability in 2020 by announcing that it would investigate legislative means to pressure online marketplace into doing more against the phenomenon of counterfeits sold via their services. It would look into the possibility of expanding contributory trademark infringement standards to online platforms.[1497] Given the US tradition so far to absolve online marketplaces from even less onerous duties than stipulated elsewhere in the world, this is a remarkable step. It is further proof of the mounting policy pressures on online intermediaries to become more responsible actors.

D. Product and food safety regulation

6. Product safety (non-food products)

I. Background – product safety in e-commerce and online platforms

The sale of unsafe or non-compliant products via online marketplace and other intermediaries has received much less public policy attention than

1492 Platform-to-business (P2B) Regulation 2019/1150 (n 1248) Article 5.
1493 Omnibus Directive 2019/2161 (n 1249) Article 6a (1) (a).
1494 ibid Article 6a (1) (b).
1495 European Commission DSA proposal (n 10) Article 5 (3).
1496 ibid Article 22.
1497 'Combating Trafficking in Counterfeit and Pirated Goods - Report to the President of the United States' (n 1363) 33.

for example the issues of hate speech or copyright infringements. However, the fight against the sale of unsafe consumer products is an affirmed part of the Commission's broader initiative to tackle illegal content online and enhance the responsibilities of online platforms. According to this, the violation of product safety rules is part of the array of unlawful content that falls under the ECD's horizontal liability framework and for which online intermediaries should take more responsibility.[1498] Data from the OECD testifies to this growing problem, which correlates with the rise in e-commerce and its expansion into almost any retail category. A 2016 OECD study found that banned, recalled or incorrectly labelled products sold online are more likely to be found on e-commerce platforms than on online retailer websites.[1499] For example, in a sweep of 291 banned or recalled products in 17 OECD jurisdictions (of which 11 in the EU) the OECD found that 86% were still available via e-commerce marketplaces. This concerned safety equipment, sports products, personal care and children's products. Meanwhile, 50% of the 62 products investigated by the study did not meet safety standards, but were nevertheless available via online marketplaces.[1500] Incorrect product labelling is another frequent problem on online marketplaces. It concerned 92% of products targeted by the OECD exercise. The UK consumer association *Which?* found that unsafe children's car seats, smoke alarms, toys, USB chargers and travel adapters where routinely available via marketplaces like *eBay*, *Amazon*, *AliExpress* or *Wish.com*. Moreover, once delisted, many of these offers reappeared within days on these sites. The report also quotes research from the *Danish Consumer Council* highlighting problems with unsafe cosmetics sold via online marketplaces.[1501] Within the EU, national market surveillance authorities (MSAs) like the German *Bundesnetzagentur* (Federal Networks Agency), for example, which is responsible for enforcing compliance with consumer electronics, had identified 3.5 million products sold online that violated EU product standards. This authority routinely sweeps the sites of both e-retailers and online marketplaces. Its 2019 annual report indicates that the availability of illegal products such as frequency jammers or other formally

1498 European Commission, 'COM (2017) 555 Final' (n 69) 3, 6.
1499 OECD, 'OECD' (n 173).
1500 ibid 18–19.
1501 Which?, 'Online Marketplaces and Product Safety' (2019) Policy Paper November 2019 <https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces> accessed 3 July 2020.

non-compliant radio equipment, like mobile phones, Bluetooth speakers or drones is a persistent problem. [1502]

Like in the area of trademark infringement via online marketplaces, the reasons for this can be seen in the ground-breaking change in the supply chain and consumer behaviours caused by the internet and globalisation. Online marketplaces have become the window through which consumers can access a sheer endless variety of products from anywhere in the world and have them delivered home. All this happens through bypassing traditional import and shipping routes through the use of small postal consignments or FSPs, which are difficult to control. In this context, there is a strong link between counterfeits and product safety issues: infiltration of the supply chain happens though the same methods. In addition, counterfeit products are also more prone to carry safety and health risks. This has been described abundantly.[1503] According to the *Which?* survey mentioned above, 70% of marketplace users would support legislative changes that see online marketplaces take over a legal responsibility for overseeing the safety of products sold through their platforms.[1504]

In July 2017, the Commission acknowledged in its Notice on the market surveillance of products sold online[1505] that e-commerce posed mounting challenges to the protection of consumers. The document highlights a number of developments that pose challenges to the effective enforcement of product safety laws. It expresses a number of concerns, such as: difficulties of MSAs to trace products sold online and identify responsible economic operators; a rise in sales from e-commerce business, including marketplaces, that are located outside the EU; market surveillance authorities' problems to get access to products for testing and risk assessments; difficulties in coordinating online market surveillance activities across the EU; low consumer awareness when it comes to e-commerce purchases.[1506]

1502 Stephan Winkelmann, 'Statistik Der Marktüberwachung 2019' (Bundesnetzagentur 2020) 10–15

1503 Ohly, 'Counterfeiting and Consumer Protection' (n 1406) 35–36; European Commission, 'Summary Response - IPR Enforcement' (n 173) 10, 41; 'Combating Trafficking in Counterfeit and Pirated Goods - Report to the President of the United States' (n 1363) 16–17; Koch (n 173) 353–355; OECD and European Union Intellectual Property Office (n 1356); Union (n 1360) 36; Market Surveillance Regulation Recital 17.

1504 Which? (n 1500) 17.

1505 European Commission, 'Commission Notice on the Market Surveillance of Products Sold Online (2017/C 250/01)' (European Commission 2017).

1506 ibid 2.

II. EU product safety law and e-commerce

a. The New Approach and the New Legislative Framework

The large majority of non-food consumer products are regulated by the *New Legislative Framework (NLF)*[1507] Directives, which evolved out of the *New Approach*. This regulatory area is different from the previous fields of intellectual property, which concerned mainly economic rights, enforced chiefly through private law. Likewise, defamation and hate speech[1508] are essentially private law areas that have personality rights at their centre. In that respect, only the fight against terrorism shares its public law focus with the area of product (and food) safety, where both the substantive law and its enforcement provisions are regulated by EU or national public law.

The General Product Safety Directive (GPSD)[1509] and Regulation 765/2008[1510] on market surveillance are the two centrepieces of product regulation in the EU. The GPSD sets out the safety requirements of products and the responsibilities and obligations of economic operators and Member States to meet these requirements. This includes provisions on how to deal with dangerous products and product recalls. The GPSD is complemented by *lex specialis* in certain product sectors. These specific directives set out additional, harmonised technical safety requirements in order to address risks that these products pose to consumer and public health. For example, toys need to meet certain enhanced requirements when it comes to the chemical composition of products, product design (such as detachable small parts), or warning labels etc. Regulation 765/2008 deals mainly with the enforcement of the provisions laid down in the GPSD and the sector specific product laws. It provides more detailed definitions of economic operators (manufacturers, importers, distributors)[1511] and spells out the responsibilities of national MSAs in the enforce-

1507 European Commission, 'New Legislative Framework - Growth' (n 22).

1508 With the notable exception where hate speech impacts the public safety and security interests at national level and for the EU under the area of 'freedom, security and justice'. Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law Recital 2.

1509 Directive 2001/95 (GPSD).

1510 Regulation (EC) 765/2008 of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products 2008 (OJ L 218).

1511 ibid Article 2.

ment of product sector laws.[1512] This Regulation was supplemented in 2019 by the Market Surveillance Regulation 2019/1020[1513] (MSR). It was passed as part of the EU Goods Package, which aims to strengthen the horizontal enforcement of EU product safety rules in the face of e-commerce and the fragmentation of national MSAs' activities.[1514]

In order to understand the more structural problems of the enforcement of product regulation with regards to e-commerce and online intermediaries a brief overview of the history of the *NLF* and the *New Approach* is appropriate. The *New Approach* was instigated in 1985[1515] as a consequence of the CJEU's *Cassis de Dijon* ruling.[1516] In this decisive case a German retailer wanted to market French fruit liqueur in its German retail outlets. The German authorities refused the retailer to market the product because domestic legislation required that fruit liqueurs have a minimum alcohol content of 25%. The French product had between 15 – 20% of alcohol content. The German Government cited the general interest reasons of public health and consumer protection against unfair commercial practices[1517] for imposing these restrictions. The CJEU, however, found that these general interest reasons had been unjustly applied, leading to an undue restriction in the free movement of goods. The ruling had two consequences that led to the emergence of the *New Approach* to product legislation.

1) The general interest exemptions that allow for a restriction to the free movement of goods must be applied in a proportional way. As a result, the EU legislator started to define the general interest, or essential requirements, through legislation in various product areas. The idea behind the harmonisation of these essential requirements was to remove any possibility that Member States unilaterally apply restrictions on products on the ba-

---

1512 For a more detailed overview of the interplay between *lex specialis* and the framework legislation of the GPSD and Regulation 765/2008 see: Lauren Sterrett, 'Product Liability: Advancements in European Union Product Liability Law and a Comparison Between the EU and U.S. Regime' (2015) 23 Michigan State International Law Review 885, 42.

1513 Market Surveillance Regulation.

1514 European Commission, 'The Goods Package: Reinforcing Trust in the Single Market, COM(2017) 787 Final' (2017).

1515 Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards 1985 (OJ C 136).

1516 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*, *Case 120/78* [1979] EU:C:1979:42 (CJEU).

1517 ibid 9.As provided for in: Treaty on the Functioning of the European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2016) Article 36.

sis of their general interest. The essential requirements relate mainly to health and safety risks of certain products. Meeting the essential requirements means that the products can be freely marketed across the EU.[1518] Under this kind of approach, the EU has, for example, put in place legislation that fixes essential technical (safety) requirements for electronic products (e.g. electromagnetic compatibility[1519], wireless communication[1520]), toys[1521], protective equipment[1522] or medical devices.[1523] The EU uses Article 114 TFEU, which gives it competence to approximate laws in the interest of the functioning of the single market, as a legal basis for these initiatives.[1524]

2) *Cassis de Dijon* laid the foundations for the principle of mutual recognition.[1525] Goods which can legally be marketed in one Member State will automatically be accepted across all other Member States and the European Economic Area (EEA).[1526] If goods meet the essentially requirements spelled out in the relevant product legislation, then it does not matter where they are first placed on the market for them to be accepted throughout the Community area.

These principles gave rise to EU standardisation and the *CE* sign, the hallmarks of the *New Approach*. Essential requirements are relatively high-

1518 For more detail on the interplay of product legislation with the Treaty provisions: European Commission, 'Commission Notice, The "Blue Guide" on the Implementation of EU Products Rules 2016, (2016/C 272/01)' (European Commission 2016); European Commission (ed), *Free Movements of Goods: Guide to the Application of Treaty Provisions Governing the Free Movement of Goods* (Publ Off of the Europ Union 2010); Schepel (n 34) 63–66.

1519 Directive 2014/30/EU of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) 2014 (OJ L 96).

1520 Directive 2014/53/EU of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment 2014 (OJ L 153).

1521 Directive 2009/48.

1522 Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (Text with EEA relevance) 2016 (OJ L 081).

1523 Regulation (EU) 2017/745 of 5 April 2017 on medical devices 2017 (OJ L 117, 552017).

1524 Other product areas, such as furniture or tableware, are not subject to specific legislation, but may still be wholly or in part covered by European Norms (standards). In any case, they are still subject to the provisions of the GPSD.

1525 Friedl Weiss and Clemens Kaupa, *European Union Internal Market Law* (Cambridge Univ Press 2014) 69–71.

1526 *Cassis de Dijon* (n 1515) para 14.

level iterations that address the specific health and safety concerns of certain products groups. Meeting them involves, however, more complex technical product design considerations. Inserting these technical specifications into legislation was deemed unpractical and too inflexible given technological and market developments. The European Commission decided to put the responsibility for defining these more detailed technical specifications to standardisation bodies. These private, industry-run organisations were tasked with drawing up harmonised technical standards which incorporate the technical specifications. Meeting such technical standards provided a presumption of compliance for manufacturers that their products complied with the essential requirements spelled out in sector *lex specialis*.[1527] The standards remain largely voluntary, which means that manufacturers may, in theory, design their products to their own technical product specifications and then provide proof that they meet the essential requirements. Under the *New Approach* Directives, manufacturers need to create a declaration of conformity for their products and affix a *CE* Mark. The declaration of conformity needs to list the product directives or regulations that the product complies with. The *CE* mark serves as a demonstration to the consumer and other actors along the supply chain that the product meets the essential requirements and can be marketed in the EU.[1528]

The EU standardisation policy of the *New Approach* is seen as a success that made an important contribution to EU integration.[1529] It has been continuously reformed, formalised and expanded,[1530] covering more products and spreading into the area of services.[1531] As of today, there are over

1527 Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products 2008 (OJ L 218) Article R8.

1528 Jean-Pierre Galland, 'The Difficulties of Regulating Markets and Risks in Europe through Notified Bodies' (2013) 4 European Journal of Risk Regulation 365.

1529 Rob Van Gestel and Hans-W Micklitz, 'European Integration through Standardization: How Judicial Review Is Breaking down the Club House of Private Standardization Bodies' (2013) 50 Common Market L. Rev. 145, 156–157.

1530 Regulation 765/2008 765; Decision 768/2008 768; Regulation (EU) 1025/2012 of 25 October 2012 on European standardisation 2012 (OJ L 316, 14112012).

1531 Jean-Christophe Graz, *The Power of Standards: Hybrid Authority and the Globalisation of Services* (1st edn, Cambridge University Press 2019) 96–97 <https://www.cambridge.org/core/product/identifier/9781108759038/type/book> accessed 2 July 2020.

4,000 technical standards referenced in 30 directives or regulations.[1532] Three large EU standardisation bodies exist that continuously design new or update existing technical standards. This co-regulatory approach, whereby the public interest requirements on products are defined by legislation, but the technical details and procedures of compliance with requirements is handed over to private and society actors, has been seen as a success benefitting companies and the position of the EU as a global standard setter.[1533] This is despite potential problems and rising criticism over transparency and democratic accountability and accessibility of private standards that have ascended to become to quasi law.[1534] Within this system, enforcement lies firmly in the hands of public authorities at Member State level. This will be briefly described further below.

b. Responsibilities and liabilities of economic actors

EU product legislation has traditionally allocated the obligations for compliance with product legislation to the economic actors involved in the making available of the products on the EU market.[1535] Under the GPSD, the primary responsibility for ensuring that products are safe, lies with the person that places a product on the market, usually the producer. The producer is defined as the manufacturer, if situated within the EU, its authorised representative or any other person that affects the safety properties of the product.[1536] These economic actors would incur primary liability for any failure to comply with product safety rules. In that respect, placing on the market refers to the first time a product is made available on the EU market.[1537]

Secondly, those persons that make products available that have been placed on the market, defined as distributors, have to exercise due care when handling and marketing products. This means they need to ensure products have the required signs affixed and carry necessary documentation. They also have specific duties in reacting to any suspicions over when a product may breach compliance requirements. Once their activities affect

1532 ibid 90.
1533 ibid 95.
1534 Van Gestel and Micklitz (n 1528) 150–156.
1535 Directive 2001/95 (GPSD) Article 3 (1).
1536 ibid Article 2 (e).
1537 Regulation 765/2008 Article 2 (2). Market Surveillance Regulation Article 3 (2).

the safety of a product directly, through handling, storage or by changing its labelling, they are considered producers and primary liable.

All these requirements are fleshed out in more detail through Decision 768/2009[1538] and in sector specific legislation. For example, the Toys Safety Directive includes more detailed obligations on manufacturers regarding the traceability of toys, such as the affixation of serial or batch numbers.[1539] All actors have an obligation to cooperate with MSAs in cases where dangerous products have been identified and recalled by manufacturers and authorities. In the time following the GPSD, which was enacted in 2001, there has been a marked shift in the assignment of product compliance obligations from the type of economic actor towards specific activities, such as placing on the market. This can be seen at least partly as a result of the rise of e-commerce. The GPSD had for example not defined the concept of placing or making available on the market. But with the rise of online retail an increasing number of products where in fact placed on the market without an economic operator that resided within the EU, or by EU actors that were traditionally not seen as economic operators, such as fulfilment service providers (FSPs)[1540] or online marketplaces.

As an answer to this problem, the recent Market Surveillance Regulation (MSR) included FSPs as economic actors, with specific responsibilities. It also attempted to clarify the role of online marketplaces (referred to as ISSPs in the regulation). Finally, it stipulated that a product can only be placed on the market if there is an economic operator established in the EU.[1541] This will be analysed below.

III. Enforcement and e-commerce

a. Tackling the challenges of enforcement in e-commerce

Enforcement of product legislation is in the hands of Member States, who allocate their tasks to MSAs. Different product sectors are allocated to specific MSAs. Given the highly technical nature of standards, market surveil-

1538 Decision 768/2008 Chapter R2.
1539 Directive 2009/48 Article 4 (5).
1540 The activities of FSPs will be explained in more detail further below in this chapter.
1541 Market Surveillance Regulation Articles 3 (11, 13, 14, 15), 4, 6, 7 (2), 14 (4) (k), recitals 13, 16, 41.

lance and enforcement are often also distinctly technical exercises. In many Member States, MSAs are made up to a large part of engineers or scientists. The compliance of products often needs to be assessed and technical test reports examined and evaluated. The enforcement picture is therefore a distinctly technical and sectoral one, that may also be delegated to different administrational levels depending on the constitutional and administrational set up of Member States. This verticality has been reinforced by technological complexity and product innovation, which resulted in more complex safety risk assessments and certification requirements.

The need to improve horizontal coordination in order to achieve a level playing field when enforcing product laws and fighting non-compliant products was already recognised before the rise of e-commerce by the European Commission.[1542] Regulation 765/2008 attempted to address this through formulating general requirements on the organisation of market surveillance programs and common measures that MSAs must adopt when assessing products and dealing with economic operators.[1543] However, the rise of e-commerce quickly turned out to be a further challenge with a high impact on enforcement.[1544] A new proposal to strengthen the horizontal cooperation between MSAs, the '2013 Goods Package'[1545], failed, however, due to Member States disagreeing over the content of a proposed consumer product safety regulation.

The Commission's ex-post evaluation report of Regulation 765/2008 of 2016 initiated a new effort towards upgrading the enforcement framework. The report found that the application of the existing product safety framework under the *NLF* was adversely affected by two developments: e-commerce and budget constraints on MSAs.[1546] Regulation 765/2008 did not sufficiently address the problems caused by a fragmented and complicated market surveillance and enforcement system in the EU. MSAs have varying

1542 Technopolis Group and others, 'Ex-Post Evaluation of the Application of the Market Surveillance Provisions of Regulation (EC) No 765/2008' (2017) 7–8.

1543 Carsten Ullrich, 'New Approach Meets New Economy: Enforcing EU Product Safety in e-Commerce' (2019) 26 Maastricht Journal of European and Comparative Law 558, 565–566.

1544 European Commission, '20 Actions for Safer and Compliant Products for Europe: A Multi-Annual Action Plan for the Surveillance of Products in the EU, COM/2013/076 Final' (European Commission 2013) Action 12.

1545 European Commission, Proposal for a Regulation on consumer product safety and repealing Council Directive 87/357/EEC and Directive 2001/95/EC, COM(2013) 78 final 2013 [2013/0049/COD].

1546 Technopolis Group and others (n 1541) 102–103, 142–143.

degrees of competencies and resources across Member States. This leads to disparities when it comes to access to product testing or sanctioning powers. Cross-border cooperation between MSAs on EU level, as well as cooperation with economic actors was seen as unsatisfactory.[1547] As a purely illustrative example, there are about 500 different MSAs across the EU that enforce the *NLF* product safety laws. In some Member States, especially those with federal structures, like Germany or Spain, enforcement competencies may be at different administrational levels (Federal, regional state, or even local).[1548] If this is added to the existing funding challenges, then it becomes clear that the enforcement system is broadly inapt to deal with the many unsafe products sold online. Effective market surveillance of e-commerce requires extra close intra-EU cooperation and swift action. Existing informal networks of cooperation such as the Administrative Cooperation Groups (AdCos),[1549] or the Information and Communication System on Market Surveillance (ICSMS)[1550] have witnessed a mixed degree of adoption by Member States, leading to suboptimal efficacy. Even the RAPEX system for notification of dangerous products is used inconsistently by MSAs.[1551] The emerging picture shows the difficulties MSAs face when dealing with product safety issues online, where sellers may delete offerings; change or re-introduce them through other platforms, supply chain channels or Member States; simply disappear or are out of the jurisdictional reach of EU MSAs. These problems will be illustrated in more detail in the case studies in the next Chapter.

1547 ibid 36–72, 11–113.

1548 ibid 82–84; European Commission, 'Commission Staff Working Document -Impact Assessment - Proposal for a Regulation of the European Parliament and of the Council Laying down Rules and Procedures for Compliance with and Enforcement of Union Harmonisation Legislation on Products - SWD(2017) 466 Final - Part 2/4' (European Commission 2017) 401–458.

1549 'Administrative Cooperation Groups (AdCos)' (*Internal Market, Industry, Entrepreneurship and SMEs - European Commission*, 5 July 2016) <https://ec.europa.eu/growth/single-market/goods/building-blocks/market-surveillance/organisation/administrative-cooperation-groups_en> accessed 3 July 2020.

1550 'ICSMS - European Commission' <https://webgate.ec.europa.eu/icsms/?locale=en> accessed 3 July 2020. It is telling that that page prominently states in of its headings that "Current market surveillance practice is desperately in need of improvement."

1551 'Safety Gate: The Rapid Alert System for Dangerous Non-Food Products' <https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm> accessed 3 July 2020. For a detailed account of these problems see: Technopolis Group and others (n 1541) 66–78.

The EU aims to address these shortcomings through the creation of a Union Product Compliance Network under the new MSR. This new network is supposed to expand and strengthen the existing regulatory networks, namely the AdCos, ICSMS and RAPEX by backing them up with a centralised administrational structure.[1552] All this will be supported by an improved, binding framework for coordination of surveillance, more EU funding and enhanced powers for MSAs.[1553] In the context of the highly heterogenic state of enforcement, institutional differences and ongoing public funding crises, the EU has a Herculean task ahead.

b. Online intermediaries and product safety law

E-commerce meant that new intermediaries have entered the supply chain of consumer products. These were either entirely new actors, like FSPs or e-commerce marketplaces, or existing providers that adapted to the online environment, such as payment services or advertising intermediaries.

Fulfilment Service providers

Fulfilment service providers (FSPs) have emerged thanks to the demands of e-commerce. FSPs have answered to the demand of customised B2C order fulfilment, helping smaller, brick and mortar or online businesses to scale their e-commerce operations. They offer shipment, storage and stock management solutions, order preparation and may even handle customer returns and complaint handling or sales analytics.[1554] These services are used by sellers that operate their own websites and those selling on online marketplaces. FSPs have helped to democratise e-commerce by enabling small shops to sell potentially worldwide, by offering affordable and easy-to-manage shipping and storage solutions.[1555] On the more controversial side, FSPs have often been identified by MSAs as fulfilling goods on behalf of sellers based outside the EU. However, they were not identified as economic operators under the existing product safety rules prior to the MSR.

1552 Market Surveillance Regulation Articles 29 - 35.
1553 ibid Articles 13 - 16.
1554 C Dwight Klappich and others, 'Warehousing and Fulfillment Vendor Guide' (Gartner 2018) Research Note.
1555 Ullrich, 'Déjà vu Davidoff – The German Federal Court of Justice Refers Another Case Brought by Coty Dealing with Trade Marks in e-Commerce to the CJEU' (n 593) 6.

Both the EU Blue Guide and the Commission Notice concluded that, depending on the activities of the FSP, they could be categorised as distributors, importers or authorised representatives under Regulation 765/2008 and the GPSD.[1556] The Commission noted the legal uncertainty relating to FSPs when it came to enforcing product safety rules and recommended that they be included as economic actor during the drafting phase of the MSR.[1557]

The MSR now includes FSPs as a new category of economic operators if they are engaged in at least two of the following four activities: warehousing, packaging, addressing and dispatching. It is noteworthy that the definition in the MSR clearly distinguishes them from pure postal, parcel or freight delivery services.[1558] It offers therefore a more realistic characterisation than the one accepted in the trademark infringement case *Versand durch Amazon* by the BGH mentioned previously. An FSP would have primary, manufacturer style obligations, if they are the sole economic operator for that product within the EU, i.e. they are placing it on the market. Apart from that, they would in any case have distributor due care obligations of: verifying the existence of applicable product compliance documentation, being at the disposal of MSAs for information and cooperation requests, and informing MSAs where they suspect that a product presents a risk.[1559] The MSR therefore allocates clear obligations to FSPs and gives MSAs a legal basis to enforce product safety rules.[1560] The solution found for online marketplaces differs somewhat in that respect.

Online intermediaries as economic actors prior to the Market Surveillance Regulation

Online marketplaces have seen a phenomenal rise. From global operators *Amazon*, *Alibaba* and *eBay*, sector specific or emerging sites like *Asos*, *Etsy*

1556 European Commission, 'Blue Guide' (n 1517) 36; European Commission, '2017/C 250/01' (n 1504) 7.

1557 European Commission, 'Commission Staff Working Document -Impact Assessment - Proposal for a Regulation of the European Parliament and of the Council Laying down Rules and Procedures for Compliance with and Enforcement of Union Harmonisation Legislation on Products - SWD(2017) 466 Final - Part 1/4' (European Commission 2017) 22–25, 125.

1558 Market Surveillance Regulation Article 3 (11).

1559 ibid Article 4.

1560 Whether this will happen effectively in reality depends on the MSA in question and their ability to cooperate with other MSAs and economic operators.

or *Wish*.com, to regional or national players, such as *CDiscount*, *PriceMinister*, *Allegro*, *Frubit*, *Emag* or *Shopping24*, an impressive variety of online marketplaces exist today. In addition, social media companies like *Facebook* or *Google* have also forayed into e-commerce, founding their own marketplaces, while other social media or messaging networks like *WhatsApp*, *Instagram*, *Twitter or Snapchat* offer in-app product purchases. Entirely new technologies, such as voice-based retail, will further change the face of e-commerce.[1561] The EU's ex-post evaluation of Regulation 765/2008 highlighted the problems of MSAs when attempting to enforce product regulation *vis-à-vis* these channels. It is increasingly difficult to pin down the role that online marketplaces play within a supply chain that has become more and more complex.[1562]

As has been seen from the area of trademarks, online marketplaces are habitually classed as online intermediaries under the ECD. The Commission Notice acknowledges that e-commerce platforms cannot be obliged to check on a general basis their marketplaces for unlawful products, because they are protected by the liability exemptions of the ECD.[1563] Consequently, they have also not been classed as economic operators under both the GPSD or Regulation 765/2008. Since they are merely required to remove and prevent specific infringing content after being notified, MSAs face the almost impossible job of seeking out infringing products on e-commerce marketplaces and file NTD requests. While in the area of unlawful speech or IP rights the damaged party or rightsholders will normally do this, this task rests almost entirely on the shoulders of MSAs, or possibly, consumer associations. As an additional complexity, violations in the area of product safety compliance are often difficult to assess. While some MSAs in Europe have been cooperating with large e-commerce platform operators, these kinds of initiatives are entirely voluntary and do normally not cover the variety of smaller or specialised marketplace operators. Still, even this proactive cooperation remains patchy, as will also be shown in the case studies.

As a result, the debate over more proactive responsibilities of these platforms has squarely entered the area of product safety. Both the ex-post evaluation and the Impact Assessment of the MSR show that some MSAs had asked for more incisive enforcement tools to penalise uncooperative online platforms that continuously sold unlawful products. They also pushed for including online platforms in the list of economic operators in the MSR,

1561 'How Conversational Commerce Is Changing E-Commerce' (n 212).
1562 Technopolis Group and others (n 1541) 90.
1563 European Commission, '2017/C 250/01' (n 1504) 10.

with the view to making them more accountable for product safety, and also argued for an amendment of the ECD on these lines.[1564]

Some Member States have attempted to formulate obligations for online intermediaries in their national product sector laws. In the national transpositions of the Radio Equipment Directive (RED) and the Electromagnetic Compatibility Directive (EMCD), Germany gave its MSA powers to demand information and support in the exercise of its duties from any economic actors that "facilitates the distribution" of products falling under the scope of these laws.[1565] The MSA is authorised to enter the premises of the economic actor and temporarily seize products for the purpose of having them tested. While this may be useful *vis-à-vis* FSPs, a more generally worded obligation to support MSAs in their work would be useful where e-commerce marketplaces resist information requests.

No EU case law has, however, been identified to this date that addresses the availability of unsafe or non-compliant products on online marketplaces.[1566] Two cases in the US indicate that marketplaces could be found liable for the sale of unsafe products under certain circumstances. In May 2019, *Amazon* made a legally binding agreement to sell only children's schools supplies and jewellery on its marketplace for which sellers had provided lab test reports and other proof that their products are not toxic. This followed an investigation that revealed over 18,000 purchases of products with unlawful levels of lead and cadmium on its US marketplace, including children's school lunch boxes and pencil cases.[1567] In another 2019

1564 Technopolis Group and others (n 1541) 165–167; European Commission, 'Goods Package Proposal - Impact Assessment 2/4' (n 1547) 125, 447.

1565 Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) 2016 Article 29; Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (FuAG) 2017 Article 31. The competent MSA for these two directives in Germany is the Bundesnetzagentur (BNetzA) (Federal Networks Agency).

1566 Apart from complaints by a consumer association, which has not reached the courts so far: '"Eau et Rivières de Bretagne" porte plainte suite à la vente de pesticides aux particuliers par Amazon et eBay' (*France 3 Bretagne*) <https://france3-regions.francetvinfo.fr/bretagne/ille-et-vilaine/rennes/eau-rivieres-bretagne-porte-plainte-suite-vente-pesticides-aux-particuliers-amazon-eBay-1748271.html> accessed 3 July 2020.

1567 Washington State, Office of the Attorney General, 'AG Ferguson: Amazon Must Remove Toxic School Supplies, Kid's Jewelry from Marketplace Nationwide | Washington State' (19 May 2019) <https://www.atg.wa.gov/news/news-releases/ag-ferguson-amazon-must-remove-toxic-school-supplies-kid-s-jewelry-marketplace> accessed 3 July 2020.

case, an US Appeals court denied *Amazon* the protections of the CDA.[1568] The judge found that the marketplace's role in the transaction was more than mere editorial, due to the fact it charges a commission, and offers storage, packaging and delivery services to sellers against an extra fee. It could therefore be held liable. A woman had bought a retractable dog leash from a seller. The dog leash had recoiled, permanently blinding the woman in one eye. The seller subsequently disappeared from the site without a trace.

However, the case studies in Chapter 5 will also show that there is normally little appetite on the side of MSAs to bring marketplace operators to court for a lengthy test case when they need to rely on cooperation to get their daily issues of unsafe products addressed. MSAs routinely approach e-commerce platforms for details of sellers that sell unsafe or non-compliant products, a task which can easily drag out if there are no informal and well working arrangements with platforms. In addition, the ex-post evaluation report of Regulation 2008/765 also shows that MSAs have widely varying enforcement powers when it comes to taking off illegal content from a website. In Spain, Germany, Italy, Belgium, Austria, Ireland, Poland or Sweden, MSAs have virtually no or very few powers to remove unlawful content from websites. As per the ex-post evaluation report, only Slovenian MSAs had the power to remove illegal product offers from websites throughout all of the 33 non-food product sectors surveyed.[1569] Even where they exist, the enforcement options via online sales channels is fragmented and fraught with practical difficulties.[1570] This was confirmed by the case studies in the next chapter. This piecemeal approach is clearly ineffective.

The Market Surveillance Regulation 2019/1010 (MSR)

The MSR includes ISSPs for the first in a piece of product safety legislation.[1571] Recital 16 clarifies that the EU lawmakers had online platforms in mind "which offer intermediary services by storing third party content, without exercising control over that content, and therefore not acting on behalf of an economic operator." Unlike FSPs, ISSPs are, however, not defined as economic operators in the MSR. Moreover, the application of the intermediary liability exemptions of the ECD is confirmed by the MSR,

1568 *Oberdorf v Amazon.com Inc* [2019] Third Circuit Court of Appeals 18-1041.
1569 Technopolis Group and others (n 1541) 74, 210–211.
1570 ibid 74, 159–167.
1571 Market Surveillance Regulation Article 3 (14).

with a special emphasis being put on the actual knowledge criterium.[1572] This does, however, not answer the question over the status of online marketplaces under product safety law, if they are found to fall foul of the ECD protection criteria, by e.g. not acting on actual knowledge along the due diligent economic criteria established in *L'Oréal v eBay*. In such a scenario, the current definitions of economic operators would still exclude them from any further reaching responsibilities. It should nevertheless be mentioned that in contrast to Regulation 765/2008 and Decision 268/2008 the definition of economic operators in the MSR is an open one. Apart from manufacturers, authorised representative, importers, distributor and FSPs, it now also includes "any other natural or legal person who is subject to obligations in relation to the manufacture of products, making them available on the market or putting them into service in accordance with the relevant Union harmonisation legislation."[1573] Whether this could potentially cover ISSPs will be discussed further below.

MSAs are now explicitly authorised to make use of the possibilities offered by the ECD to restrict access to an 'online interface'[1574] operated by a trader that did not comply with an order to remove infringing content or display warnings to end users.[1575] This provides wider enforcement tools to MSAs, but given their limited experience and reluctance in this area so far, it remains to be seen how fast and how efficient this can be implemented. In addition, it would potentially require these 500+ MSAs to engage with online marketplaces directly and, if needed, with the national authorities responsible for enforcing the ECD according to the country-of-origin principle. To complicate things further, courts may also be brought into the picture if content removal orders are deemed to be applied disproportionately. The doubts over the efficacy of content blocking and the possibilities of sellers to market their products elsewhere throws further shadows over this new enforcement opportunity.

The second, arguably more important obligation of ISSPs, is that they need to work together with MSAs in specific cases and facilitate action to

---

1572 ibid Article 2 (4), Recitals 16, 41, 42.

1573 ibid Article 3 (13). Which refers to any additional requirements imposed by requirements

1574 The definition of online interface has been carried over from the Geo-Blocking Regulation. It offers a technology neutral definition of a website, which is operated by or on behalf of a trader and that gives customers access to its products or service. In the context of the Market Surveillance Regulation this appears to refer mainly to the online shopfronts of retailers.

1575 Market Surveillance Regulation Article 14 (3) (k).

eliminate or mitigate risks presented by a product offered for sale through their sites.[1576] The language here is clearly kept to specific, singular circumstances, so as to disperse any suspicion that online marketplaces could be harnessed by MSAs for broader proactive measures aimed at preventing unsafe products, which could violate the ECD's Article 15. Article 7 (2) of the MSR will nevertheless help MSAs to get online marketplaces to cooperate more readily where it concerns information requests on products, sellers, or conduct test purchases. It could also be used to help MSAs engage marketplace operators to display online warning messages to consumers where it concerns risky product offers. The MSR, however, merely mentions the tools that already exist under the ECD against online marketplaces.

As stated in the section on trademarks, EU regulation in the area of consumer protection against uncommercial practices (UCPD) appears to go further. The Guidance Note of the UCPD gives a useful indication of the direction that accountability for the integrity of products sold via marketplaces could take. It reiterates the fact that the ECD applies without prejudice to the level of protection of interests relating to public health and consumer protection. It therefore serves as a complement to the EU consumer acquis.[1577] Online platforms that fall under the definition of a trader under the UCPD would therefore need to apply standards of professional diligence that correspond to the activity of the platform/trader.[1578] According to the UCPD, the definition of trader includes anyone who acts in the name of or on behalf of a trader.[1579] Meanwhile, B2C commercial practises under the directive include any act "directly connected with the promotion, sale or supply of a product to consumers."[1580] This, it could be argued, is similar to the commercial communication requirement in trademark law. It is hardly questionable that today's online marketplaces are not conducting activities that would qualify them as such traders. This could mean they are held to "designing their web-structure in a way that enables third-party traders to present information to platform users in compliance with EU marketing and consumer law."[1581] According to the

1576 ibid Article 7 (2).
1577 European Commission, 'UCP Directive Guidance' (n 57) 126.
1578 ibid 126–127.
1579 Directive 2005/29/EC Article 2 (b).
1580 ibid Article 2 (d).
1581 European Commission, 'UCP Directive Guidance' (n 57) 126.

UCPD guidance, platforms that fail to comply with this requirement could forfeit their intermediary liability exemption.[1582]

The 2019 Omnibus Directive appears to settle this ambiguity. It clarifies that online marketplace are considered as traders in their own right, and therefore subject to professional diligence standards.[1583] While professional diligence as per the UCPD's definition is dependent on more fluid criteria of good faith and/or honest market practices, it is nevertheless tied to "a standard of special skill and care which a trader may reasonably be expected to exercise."[1584] It is submitted here, that the professional diligence of online marketplace operators could extend towards online labelling and information or registration requirements under certain product or food laws. Online marketplaces are not only (essential) technical facilitators for third-party product offerings, but also increasingly provide additional value added services to sellers or non-professional traders. They are in a central and powerful position and, at a minimum, able to provide sellers with the technical tools to adhere to information requirements and verify compliance with these rules on their sites. This information link between third-party sellers and marketplace operators is also acknowledged by the fact that under the Omnibus Directive marketplaces need to clearly indicate to customers whether a third party acts as a (professional) trader or not.[1585] This confirms a trend of both legislators and the CJEU to take an expansive view of the concept of trader when it comes to protecting consumers. This dates back to at least the 2016 CJEU judgement in *Sabrina Wathelet v. Garage Bietheres*.[1586] The CJEU found that failure by a commercial intermediary to indicate to a customer that the party offering a good for sale was an individual, meant that the intermediary could be seen as the seller under the terms of the Consumer Sales Directive.[1587] This included liabilities for any failure to comply with the terms of the sales contract.[1588] Beyond this, however, the interplay between the UCPD and the ECD in the area of product safety is as unconfirmed as in the area of IPRs,

1582 ibid 126–127.
1583 Omnibus Directive 2019/2161 (n 1249) Article 3.
1584 Directive 2005/29/EC Article 2005/29.
1585 Omnibus Directive 2019/2161 (n 1249) Article 3 (4).
1586 *Sabrina Wathelet v Garage Bietheres & Fils SPRL, C-149/15* [2016] ECLI:EU:C:2016:840 (CJEU).
1587 Directive 1999/44/EC of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees 1999 (OJ L 171).
1588 *Wathelet* (n 1585) para 34.

especially trademarks.[1589] The current review of the GPSD, which will be discussed below, may provide an opportunity to lay down more adequate responsibilities for online marketplaces and other platforms that facilitate the marketing and sale of products.

Whether the MSR's open definition of economic operators may provide flexibility for *lex specialis* to include online marketplaces is unclear. The Toys Safety Directive, as one example of the 70 product rules under the MSR's scope,[1590] requires that statutory warning labels be displayed in a clearly visible way online before the consumer makes a purchase decision.[1591] Under EU energy-labelling regulation, a dealer would have to make the energy label and a product information sheet available to customers, including in online distance sales.[1592] Although these obligations apply to manufacturers, distributors, or dealers, online marketplace undeniably have a special role in providing the technical infrastructure so that sellers can comply with these labelling and display requirements. Modern enforcement of product safety regulation should account for the fact, that today's online marketplaces provide virtually all information displayed on their website in a structured and measurable way. Sellers or non-professional traders are already required to upload product information, including photos and product data, in structured formats onto many marketplaces.[1593] Online marketplaces employ site merchandising teams and sophisticated analytics to maximise revenue from the displays on their websites. Where products are subject to mandatory labelling requirements, online platforms should at least have some due care requirements similar to what can be expected from dealers (e.g. under the Energy-labelling Regulation) or distributors. This would mean stretching some of the *lex specialis* economic operator categories, but this does not seem unrealistic given the integrated functionalities of online marketplaces. As stated above, these kinds of possibilities do exist already under the UCPD's and the Omnibus Directive's professional diligence requirements.

To summarise, while providing little direct enforcement means against online marketplaces, there are still some improvements under the new MSR that may help MSAs. First, the open economic operator definition

1589 Moscon and Hilty (n 1422) 12–15.
1590 Market Surveillance Regulation Annex I.
1591 Directive 2009/48 Article 11 (2); European Commission, 'Toy Safety Directive 2009/48/EC - An Explanatory Guidance Document Ref. Ares(2016)1594457' (n 441) 42.
1592 Regulation 2017/1369 Article 5 (1).
1593 Ullrich, 'New Approach Meets New Economy' (n 1542) 576.

may give room for drawing online platforms into its scope in product sectors covered by *lex specialis*. Secondly, MSAs can require that online marketplaces cooperate in specific cases to eliminate or mitigate product safety risks. Third, MSAs have received clarification that they can approach ISSPs to block access to infringing offers. A more ambitious consideration of the role online marketplaces play in the supply chain and the impact they have on product safety, as was done for FSPs, would have been appropriate, however. Marketplaces that are not protected under the ECD due to their active role would currently be in a grey zone between these two legal frameworks.

IV. Private enforcement

Little is publicly known about online marketplaces' voluntary activities in the area of product safety. The reactive duties under the ECD restrict their obligations to removals and possibly stay-downs following an NTD request. They are theoretically not even obliged to act on public product recalls unless they are notified of recalled products on their sites. The websites of the large marketplaces as of today only refer to their terms and conditions, which forbid sellers to list products that are non-compliant, unsafe or recalled.[1594] Larger marketplaces may have monitored or checked whether public recalls are being complied with by sellers on their sites, or whether sellers are subject to product safety escalation from customers, but again, little is known on this.

On 25 June 2018, the European Commission and online marketplaces *AliExpress*, *Amazon*, *eBay* and *Rakuten France* initiated the Product Safety Pledge.[1595] Under the Product Safety Pledge, online marketplaces made voluntary commitments to consult public recalls websites from the EU and MSAs and remove recalled products from their sites. The platforms also commit to react to MSA notices within two days, and to customer notifications of product safety issues within 5 days. For that, they vow to put in place effective NTD systems for unsafe products, where not done so already. The commitments also include sanction processes for repeat offenders and the prevention of relistings of removed product offers. On the

1594 For example: 'Product Safety Policy' (*eBay*) <https://www.eBay.co.uk/help/policies/prohibited-restricted-items/product-safety-policy?id=4300> accessed 6 July 2020.

1595 European Commission, 'Product Safety Pledge' (n 542).

proactive side, marketplaces will nominate single points of contact for MSAs, and inform and train sellers on EU product safety rules. They also agreed to explore the potential of using technologies to detect unsafe products. Although the last point remains vague, the Pledge may illustrate the rising pressure on platforms to take more responsibility. Two KPIs will measure the processing times of MSA notices and the number of removals of unsafe products spotted by platforms through monitoring the EU RAPEX System (now the Product Safety Gate). The initiative follows the models of other voluntary codes of conduct in the areas of hate speech or counterfeiting.

The latest progress report on the Pledge, covering the period from April to September 2019, showed that the original signatories had complied with the 2-day removal deadline of identified and notified unsafe products in approximately 95% of cases.[1596] Two of the participating platforms shared that they had messaged and trained sellers on product safety rules, albeit without providing any more data on this activity. The platforms indicated that they use a mix of proactive technologies to identify and block unsafe and non-compliant products, which included block filters, internal risk analysis and machine learning tools based on historic, internal data. Two additional marketplaces (*Allegro* and *CDiscount)* have since joined the agreement.

Despite its general wording, the initiative demonstrates that online marketplaces are in a key position to affect product safety on their platforms. The commitments of the Product Safety Pledge understate, however, the role of platforms. Seller education, seller onboarding due diligence and sanctioning can be key processes to limit the sale unsafe and non-compliant products. Risk analysis and proactive identification mechanisms have the potential to be effective if used holistically, e.g. by incorporating data gathered by platforms on sellers, product characteristics, customer reviews and product returns or complaints records. The measures taken by platforms remain largely in the dark. This maybe partly because online marketplaces fear being held liable under the ECD for gaining actual knowledge from any proactive analysis and outreach to sellers. On the other hand, it can be argued that the current responsibilities and voluntary measures are far below what online marketplaces can and should be doing in

1596 European Commission, '2nd Progress Report on the Implementation of the Product Safety Pledge' (2019) <https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-rules_en> accessed 6 July 2020.

order to stem the flood of unsafe and unlawful products sold. More transparency and accountability would also mean that MSAs provide input and assess the measures taken by platforms. The public market surveillance and enforcement system that is characteristic of the *New Approach* and product regulation means that MSAs retain valuable technical information and surveillance expertise that may benefit platforms in their risk assessments. In addition, while the Pledge includes major European online marketplaces, it still misses a number of important market players and also does not consider the rising importance of social media marketplace activities. It covers therefore only the most visible players, but misses business models that are increasingly coming into the focus of MSAs.[1597]

V. EU legislative initiatives

On 23 June 2020, the European Commission launched an initiative to review the GPSD by opening a public consultation. The inception impact assessment outlines two major reasons for the review: 1) the 20-year-old directive does not sufficiently address the fact that new technologies, such as artificial intelligence or the Internet of Things influence product safety; 2) new challenges to product safety that are posed by e-commerce need to be tackled. In addition, the GPSD is not fully in line with the new market surveillance rules established by the MSR.[1598] This overview will focus on point 2). The Commission notes the emergence of new online business models, such as marketplaces, and states that the product safety rules applicable to them are unclear. It refers to the ECD and the Commission's 2018 Recommendation, which calls for enhanced responsibilities of online platforms.[1599] It also hints at the unsatisfactory progress under the voluntary Product Safety Pledge, to which many actors have not participated and which has not been effective enough in addressing product safety concerns. Apart from the obvious public health concerns, this also creates an uneven playing field between economic operators. It also cites the ongoing

1597 Winkelmann (n 1501) 22–25, 29. In this report, marketplace www.wish.com was mentioned as an actor that violated a number of product laws in Germany. The interviews in Chapter 5 show that social media and messaging apps pose rising problems to MSAs.

1598 European Commission, 'Combined Evaluation Roadmap/Inception Impact Assessment - Revision of Directive 2001/95/EC on General Product Safety - Ref. Ares(2020)3256809' (2020) 1.

1599 ibid 2; European Commission, 'C(2018) 1177 Final' (n 8).

purchase of goods online from non-EU operators as an issue that needs to be addressed more effectively.[1600] The legal basis for the initiative is provided by Article 114 TFEU. Achieving better consumer protection and a level playing field for businesses requires better cooperation of MSAs across the EU, which, because of its scale is best done at Union level. The European Commission foresees to coordinate the GPSD review with the proposed Digital Services Act.[1601]

The Commission charts out 4 policy options. With regards to action relevant for online platforms, the first Option would reinforce the current Product Safety Pledge and increase funding for joint market surveillance activities. The second and third options are scaled variants of a partial or full revision of the GPSD. They would result in making some voluntary provisions of the Pledge legally binding (Option 2), or add new obligations that go beyond the current Pledge (Option 3). Market surveillance would either be more strongly aligned across Member States, while keeping different legal instruments, or Member States would be given stronger enforcement powers, with the Commission being enabled to arbitrate in cases where risk assessments diverge. Finally, Option 4 would see an entirely new legal instrument that would incorporate Option 3 and merge the GPSD with the MSR into one set of rules.

The initiative follows the familiar procedure that was also witnessed in the area of terrorist content or copyright. Where progress based on voluntary and self-regulatory codes of conduct is not deemed sufficient, the EU wields the stick of legislative intervention. The concurrence of the GPSD review with the DSA will provide for an interesting policy making process. Enhanced responsibilities for online platforms beyond the Pledge's commitments are, it is submitted here, options that lie within the technically and morally justifiable realm. As stated before, these obligations will need to be accompanied by solid procedural rules and supervisory powers of MSAs. The area of product safety, with its strong expertise in public enforcement and standard development, could be predestined to achieve such a transparent and accountable responsibility structure for online platforms.[1602]

1600 European Commission, 'Combined Evaluation Roadmap/Inception Impact Assessment - Revision of Directive 2001/95/EC on General Product Safety - Ref. Ares(2020)3256809' (n 1597) 2.

1601 ibid 3.

1602 Ullrich, 'Standards for Duty of Care?' (n 1137) 126–127.

The DSA proposal appears to have seized on the enhanced enforcement powers created by the MSR by laying down specific requirements and due diligence obligations for online marketplaces. For one, Article 22 on the traceability of traders, in conjunction with Article 9, allows authorities to request the disclosure of information on specific service recipients (traders). This would provide MSAs with long-sought powers to gain information on traders selling non-compliant products.[1603] The fact that compliance with information orders is directly linked to the availability of the liability exemption may add additional weight to MSAs activities, as any failure to follow these orders could expose marketplaces to direct liabilities under national rules. Secondly, the requirement that marketplaces shall design their online interfaces (e.g. web pages) in a way that allows traders to comply with statutory pre-contractual information and with product safety rules[1604] imposes additional responsibility on marketplace operators. It was shown above, that online marketplaces do provide the essential technical infrastructure that can be harnessed to enable traders to comply with product safety labelling and information requirements. Under the new proposal, they would need to acquire a more in-depth understanding of product-specific safety and compliance labelling requirements online, such as on toy safety, eco-labels, chemical ingredients or food allergen warnings, in order to give traders the technical means to display this mandatory information. This appears to be more than appropriate given the key position that these actors occupy in facilitating the availability of products at a massive scale. The language in Article 22 (7) could be enhanced further by imposing specific non-compliance identification and reporting requirements on marketplace operators, similar to Regulation 2019/1148 on the marketing and use of explosives precursors,[1605] at least were it concerns areas susceptible to higher public health and safety risks. It remains to be seen whether the current GPSD review and product *lex specialis*, both in the area of food and non-food regulation, will venture further with specific obligations for online marketplaces and other online intermediaries. Under the current DSA draft, due diligence operations come closer to viewing online marketplace as economic operators with their own due diligence obligations in the supply chain of products.

1603 This is one of the main enforcement gaps reported by MSAs in the case studies in Chapter 5.

1604 European Commission DSA proposal (n 10) Article 22 (7).

1605 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors Articles 7 - 9.

VI. Summary and outlook

The rise of e-commerce and online marketplaces has also led to an increase in unsafe and non-compliant products sold by sellers via online marketplaces. The phenomenon is global and poses important risks for consumer trust and safety. Like in all the other sector treated beforehand, online intermediaries occupy a special role in this process. An increase of control of and commercial gain driven from the activities of third parties stands in contrast to the wide-reaching exemption from legal responsibilities for the content and products offers hosted and marketed through their systems. Product safety touches on public health and safety interests. Its regulatory set up differs from the private, personality law focussed-areas of defamation and hate speech and the economic and contractual rights impacted by intellectual property. Product safety law, like terrorism provisions, are enforced by public authorities. In the case of product safety law, MSAs operate in a highly technical and fragmented enforcement environment that was largely unprepared for the new problems caused by e-commerce and the rise of online marketplaces. MSAs in the EU have had marked problems to enforce product safety rules in e-commerce. Wide-reaching liability exemptions protect the only actors they often can get hold of when pursuing infringing sellers. The purely reactive duties of online marketplaces mean MSAs are facing the daily uphill struggle of searching for unsafe products on marketplaces and social media, while these powerful actors have virtually no duties.

The MSR has addressed this vacuum of responsibility only marginally, by enhancing marketplaces' obligations to cooperate with MSAs and by offering the possibility to suspend websites with unlawful products. The voluntary Product Safety Pledge has done little to alleviate regulatory concerns over consumer health and safety in e-commerce. The GPSD review, in conjunction with the DSA proposal, may finally lead to a readjustment of responsibilities for online intermediaries in this area. It is submitted here that, at least for sectors that carry higher product safety risks (e.g. toys), and where online labelling obligations exist, online intermediaries should be seen as economic actors with adequate primary or distributor liabilities. The DSA proposal has ventured to address this responsibility gap by obliging online marketplace to enable traders to display statutory product safety information. This, in conjunction with enhanced traceability requirements for traders, is an important step in bringing the responsibilities of online marketplace more in line with their economic significance and their impact on consumer safety.

The *New Approach* is based on a co-regulatory system that uses harminsed technical standards as a means to protect public interests in complex technical and dynamic market sectors.[1606] EU product regulation could be a valuable model for a new intermediary responsibility system. Chapter 6 will explore how online intermediaries could be brought into such a regulatory system.

7. Food safety

I. Background – food in e-commerce and on online platforms

Online food retail took off somewhat later than e-commerce in general. Since 2010, online food retail has, however, also started to become mainstream. The ascendance of e-commerce marketplaces can be seen as a catalyst for this trend. A 2012 survey shows that the number of unique food items offered on the german *eBay* site grew from 2,000 in 1999 to 150,000 in 2012. Amazon launched its grocery category in 2010 with 42,000 unique products, which grew to a selection over 175,000 within two years.[1607] Today, online marketplaces offer millions of food products online. In 2019, 36% of Dutch, 32% of British consumers and 25% of German consumers had shopped for grocery online.[1608] Although online grocery sales made up only 2%[1609] of the total food retail market in Europe in 2018, the sector is set to continue with double digit annual growth rates over the foreseeable future and will represent USD22 billion in the UK and USD17 billion in France by the year 2023.[1610]

The unique nature of e-commerce means that product selection online is vast and can be shipped to virtually anywhere in the world. This has given have given rise to a number of problems that are exacerbated by the techni-

1606 Jacob Rowbottom, 'If Digital Intermediaries Are to Be Regulated, How Should It Be Done?' (*Media Policy Project*, 16 July 2018) <http://blogs.lse.ac.uk/mediapolicyproject/2018/07/16/if-digital-intermediaries-are-to-be-regulated-how-should-it-be-done/> accessed 7 August 2018; Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 226.

1607 Dirk W Lachenmeier and others, 'Does European Union Food Policy Privilege the Internet Market? Suggestions for a Specialized Regulatory Framework' (2013) 30 Food Control 705, 706.

1608 'Europe: Online Grocery Market, by Country 2006-2019' (*Statista*)

1609 In advanced markets like the UK this share 10%.

1610 'Grocery Sales by Channel in Europe 2018' (*Statista*).

cally complex, tightly regulated and diverse landscape of food retail. EU food safety authorities (FSAs) have become alert to the problems of online food retail since at least 2007. A German study of that year found that of 300 slimming products test-purchased via the internet, 50% were not compliant with EU legislation.[1611] Nutritional supplements (e.g. slimming pills, sports nutrition), novel foods[1612] or foods with ingredients not authorised in the EU are of particular concern in online retail.[1613] In its 2017 Coordinated Food Control Plan on the official control of certain foods marketed through the internet, the European Commission singled out these product categories for a targeted controls exercise. During an EU wide check of 1077 websites, it found altogether 779 non-compliant supplements and novel foods from 734 traders based within and outside the EU. Many of these acted merely as intermediaries (i.e. brokers) that initiated sales through other channels.[1614] This is confirmed by a study of the German Federal Office of Consumer Protection and Food Safety (BVL), which found that sales brokered through messages on sites like *Facebook*, *Pinterest* or *Instagram* are more and more frequent.[1615] Other commonly identified problems relate to unrestricted sales of alcoholic beverages, incorrect or insufficient food labelling, unlawful health claims and microbiological risks relating to the sale of perishable or cold-chain products.[1616]

This phenomenon has led experts to claim that food regulation in online commerce is less rigorously enforced than in traditional supermarkets

---

1611 Bundesamt für Verbraucherschutz und Landwirtschaft (BVL), 'BVL/FLEP Conference on European Approaches to Risk Based Official Controls in Food Businesses, Including e- Commerce'

1612 European Commission, 'Novel Food' (*Food Safety - European Commission*, 17 October 2016) <https://ec.europa.eu/food/safety/novel_food_en> accessed 9 July 2020.

1613 'Amazon Warns Customers: Those Supplements Might Be Fake' *Wired* <https://www.wired.com/story/amazon-fake-supplements/> accessed 9 July 2020.

1614 European Commission, 'The First EU Coordinated Control Plan on Online Offered Food Products - Analysis of the Main Outcome of the Implementation of the Commission Recommendation on a Coordinated Control Plan on the Official Control of Certain Foods Marketed through the Internet, Ref. Ares(2018)893577' (2018) 2. See also Lachenmeier and others (n 1606) 709.

1615 Bundesamt für Verbraucherschutz und Landwirtschaft (BVL), 'Gemeinsame Zentralstelle "Kontrolle Der Im Internet Gehandelten Erzeugnisse Des LFGB Und Tabakerzeugnisse" - Jahresbericht 2018' (2019) 8 <https://www.bvl.bund.de/DE/Aufgaben/06_Onlinehandel/onlinehandel_node.html> accessed 16 July 2020.

1616 Lachenmeier and others (n 1606) 707–710.

and offline high street retail. Food safety levels risk therefore being lower in online shopping.[1617]

II. Food safety and its enforcement in EU and national law

a. EU food safety law – responsible economic actors

EU food safety constitutes a separate regulatory regime.[1618] The EU Hygiene package[1619] is a comprehensive, technically complex and diverse regulatory system that exists since 2006. It is mainly based on regulations, which underlines the centralised and relatively unitarian character of EU food law.[1620] The responsibility for food safety spreads throughout the entire food supply chain, starting at the manufacturer and ending at the retailer. Like in the area of non-food products, the EU's regulatory choice has led to the establishment of co-regulatory practices.

The Regulation on general food law[1621] and the Regulation on the hygiene of foodstuffs[1622] set out the framework conditions by stipulating responsibilities and quality management principles, such as the mandatory use of Hazard Analysis and Critical Control Points (HACCP) or Good Hygiene Practice (GHP).[1623] The private sector manages the compliance with these principles by designing standards and certifications, an activity that is encouraged by the EU.[1624] Food safety authorities are predominantly

---

1617 ibid 706.

1618 'General Food Law - Food Safety - European Commission' (*Food Safety*) <https://ec.europa.eu/food/safety/general_food_law_en> accessed 6 July 2018.

1619 European Commission, 'Food Hygiene' (*Food Safety - European Commission*, 17 October 2016) <https://ec.europa.eu/food/safety/biosafety/food_hygiene_en> accessed 9 July 2020.

1620 Agnieszka Bilska and Ryszard Kowalski, 'Food Quality and Safety Management' (2014) 10 Scientific Journal of Logistics 351, 351–353.

1621 Regulation (EC) 178/2002 of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety 2002 (OJ L 31).

1622 ibid.

1623 Regulation 852/2004 Recital 11, Article 1 (d) (e).

1624 ibid Recital 44; Regulation 178/2002 Article 5 (3). Such standards are for example provided by ISO 9000 Quality Management or ISO 22000 Food management systems norms, International Food Standard (IFS), or the British Retail Consortium (BRC) Global Standard. All global food safety standards and norms are collected in the *Codex Alimentarius*, a compendium managed by the UN's Food and Agriculture Organisation (FAO)

tasked with market surveillance and enforcement. This happens through audits and official controls of the procedures developed by industry, and a harmonised system of official controls and registrations, established through Regulation 2017/625.[1625] They are conducted by applying a risk-based approach[1626] by which high risk areas, be they specific food product sectors, economic actors or supply chain activities, receive more frequent and intense controls. With the rise in e-commerce, Member States, which remain in charge of enforcement, have also started to control online sales channels. Enforcement activity may be less fragmented than in the area of non-food products, but as of now there is still a lack of coordination across the EU and expertise in checking and pursuing unlawful sales and operators online.[1627]

The Hygiene Package also lays down rules for areas where more direct regulatory invention was deemed more appropriate. Food Labelling requirements or sector specific provisions relating to e.g. novel foods, or organic products, as well as animal feedstuffs, are points in case. For example, in 2011 the EU adapted its laws on food information for consumers to the online environment. Food labelling requirements for online shops were aligned to those of physical shops. As a consequence, ingredients' lists, allergen warnings and certain nutritional information all need to be displayed online to give consumers information before they make a purchase decision.[1628] Online food retailers also need to register with national authorities[1629] and, depending on the nature of their business, may even need to ask for an authorisation to operate.

1625 Regulation (EU) 2017/625 of 15 March 2017 on official controls and other official activities performed to ensure the application of food and feed law, rules on animal health and welfare, plant health and plant protection products (OJ L 95) Chapter II, Articles 9 - 27. Regulation 852/2004 Article 6. For more detail on the co-regulatory character of EU food law see: Marian Garcia Martinez, Paul Verbruggen and Andrew Fearne, 'Risk-Based Approaches to Food Safety Regulation: What Role for Co-Regulation?' (2013) 16 Journal of Risk Research 1101.

1626 Regulation 2017/625 Article 9.

1627 This will be treated in more detailed in the case study within the following chapter.

1628 Regulation (EU) 1169/2011 of 25 October 2011 on the provision of food information to consumers 2011 (OJ L 304) Article 14 (1).

1629 Peter Kranz, Hannes Harms and Claudia Kuhr, 'Kontrolle der im Internet gehandelten Erzeugnisse des LFGB und Tabakerzeugnisse (G@ZIELT)' (2015) 10 Journal für Verbraucherschutz und Lebensmittelsicherheit 13, 14; Regulation 852/2004 Article 6 (2), Recital 19.

The European Food Safety Authority (EFSA) is a central scientific EU body that supports Member States with risk assessments, communications and enforcement decisions. The protection of human life and health and consumer interests are the general objectives of EU food law.[1630] The main regulatory tools used are harmonised risk management and the precautionary principle.[1631] Food is probably one of the most tightly regulated sectors in the EU, with a higher degree of harmonisation than in the non-food product area.[1632]

Primary responsibility for food safety lies with all food business operators. A food business is defined as "any undertaking, …, carrying out any of the activities related to any stage of production, processing and distribution of food."[1633] Food business operators have the obligation to ensure that all food under their control satisfies the relevant hygiene requirements. Depending on the kind of foods, specific requirements, like microbiological characteristics, temperature control or cold chain maintenance need to be met.[1634]

The Commission confirmed in 2016 that it deemed food regulation and online food retail to be adapted to the DSM.[1635] Online food traders are covered by the definition of food business operators. They will therefore need to follow food safety rules under general food law, including labelling and information requirements.[1636] On the enforcement side, the new Official Controls regulation empowers FSAs, amongst others, to anonymously purchase samples of products or suspend for an 'appropriate period of time' the web sites of marketplace operators that do not comply with their obligations.[1637] As forward looking actions, the Commission stated that, apart from reinforcing training of enforcement officers in e-

1630 Regulation 178/2002 Article 5 (1).
1631 ibid Articles 5 - 7.
1632 Luis González Vaqué, 'The Proposed EU Consumer Product Safety Regulation and Its Potential Conflict with Food Legislation.' (2014) 9 European Food & Feed Law Review 161, 161.
1633 Regulation 178/2002 Article 3 (2). The food business operator is the natural or legal person under whose control the food business is situated. (Article 3 (3))
1634 Regulation 852/2004 Articles 3 & 4.
1635 European Commission, 'E-Commerce Control of Food - EU Action Plan' (Advisory Group of the food chain, animal and plant health, 25 November 2016) 8 .
1636 ibid 4–5.
1637 ibid 6–7; Regulation 2017/625 Articles 36, 138 (2) (i).

commerce.[1638] it would look into establishing contact with major e-commerce platforms (*Alibaba, Amazon, eBay*).[1639]

b. Online intermediaries and food safety

The European Commission's includes the sale of food products in its broad initiative aimed at tackling unlawful content on online platforms.[1640] The above mentioned 2017 coordinated controls initiative of food sold online, which centred on nutritional supplements and novel foods, concludes that the following actions need to be taken: establishing contacts with major e-commerce platforms, including social media; seeking cooperation with payment service providers; adjusting legislation to the needs of e-commerce controls. It also admits that more needs to be done to "remind the main players of e-commerce such as platforms, payment services and the traders themselves of their responsibilities, to ask for their contributions to increase the safety of online offered foods and to reduce offers which mislead consumers."[1641]

The EU has not undertaken any official legal assessment as to what extent online marketplaces could potentially be held accountable under EU food law when allowing sellers to market food products on their platforms. Given the rising importance of online food sales, via online platforms in particular, this is surprising. Like in any other content area treated beforehand, marketplaces play an essential role in enabling the wide availability of food products to consumers. Labelling, safety and registration requirements are complex under EU food law. As mentioned in the previous section, the likes of *Alibaba* or *Amazon* provide a technical facility for the upload of products and sales offers. That facility is enriched by a wide array of other services from which the platforms derives money. A seller that has to comply with intricate online labelling requirements, would benefit from a marketplace that provides them also with the ability to display ingredients, warnings and other regulatory information in a structured way. It is submitted here that a diligent marketplace operator

---

1638 'Better Training for Safer Food (BTSF) - Food Safety - European Commission' (*Food Safety*) <https://ec.europa.eu/food/safety/btsf_en> accessed 19 April 2021.

1639 European Commission, 'E-Commerce Control of Food - EU Action Plan' (n 1634) 13.

1640 European Commission, 'COM (2017) 555 Final' (n 69) 3, 6 (fn 28).

1641 European Commission, 'Main Outcome Analysis - EU Internet Control Plan' (n 1613) 5.

would need to be aware of these specific requirements, if they chose to allow the listing of food product offers on their marketplace. This would include allowing the seller to comply with food legislation in a way that is transparent to the consumer. It would entail awareness and knowledge of the information that needs to be displayed in a given product category, and requirements to structure the layout of their sites in a way that enables a legally conform display of product information. This requirement should be commensurate to the health and safety risk related to selling food products, thus translating into an enhanced level of duty of care.[1642] Platforms would also be in a unique position to manage that risk by other due diligence measures, such as seller verification processes to check, for example, food business registrations of sellers, or online product information audits.

At the very least, today's online intermediaries have an impact on the supply chain and a certain level of control over the marketing of these products. As will be seen in the case studies in the next chapter, the view of enforcement authorities on the role of online marketplaces in e-commerce is divided. Some authorities would tend to define these actors as food business operators, where they derive a service fee or commission from sales conducted through their platforms. This ties in with the 'commercial communication' concept in trademark law.

Apart from the enhanced controls programs on the enforcement side, no further EU legal initiatives have so far been launched, and no specific private enforcement initiatives are known. It can be assumed, however, that online marketplace would cover food safety in any of the self-adopted measures that cover product safety of non-food products, like the Product Safety Pledge. Like in the area of non-food product regulation, the recent DSA proposal would enhance the enforcement options for food safety authorities in the fight against illegal and unsafe food online. Given the extensive and very specific requirements on the labelling of food sold online, Article 22 of the DSA proposal on the traceability of traders would be a welcome component for holding online marketplaces to account where they decide to enable the sale of food products. The existing registration requirements for food traders could also be directly linked to the traceabil-

1642 nutraingredients.com, 'How Responsible Is Amazon for the Supplements Sold on Its Sites?' (*nutraingredients.com*) <https://www.nutraingredients.com/Article/2015/10/09/Amazon-s-supplement-responsibility> accessed 9 July 2020.

ity obligations in the new DSA, which requires that marketplaces obtain proof that traders have registered in a public register.[1643]

III. Summary and outlook

The sale of unsafe food online belongs to the EU's broad horizontal strategy to address unlawful content via enhancing online platforms' responsibilities. The current EU Food Law framework has been adapted to some aspects of e-commerce, namely where it concerns the legal status and the responsibilities of online retailers. Labelling and registration requirements apply to these actors as much as general obligations relating to the safety of food products. The food law system itself relies on co-regulatory measures. The broad food law objectives and safety management principles are set up through regulations. These are implemented through standards and norms developed by industry. FSAs at national level, supported by an European scientific agency, EFSA, audit and control food business operators both on the ground and online. E-commerce marketplaces have, however, fallen somewhat between the cracks of this system. There is no clear view of their exact responsibilities under food law outside of the liability exemptions imposed by the ECD. The European Commission and national authorities see a need to involve platforms stronger in the fight against unsafe food products. Their essential functions are recognised, but no concrete policy action has been taken. It is suggested here, that the increasingly integrated involvement of these actors in the facilitation and promotion of food products should confer on them responsibilities that are in line with the consumer health and safety risks related to their activity, especially where it concerns online product labelling and seller registration requirements. Online platforms are certainly in a position to take on these roles. Online food labelling, consumer information and seller registration requirements could be formidable risk management tools, because they can harness the technical facility role of platforms. The EU appears to have seized, at least partly, on this opportunity in its DSA proposal.

1643 European Commission DSA proposal (n 10) Article 22 (1) (e).

E. Summary: Sectoral frameworks and intermediary liability

1. The multilevel regulatory picture of EU intermediary liability

The sectoral analysis of intermediary liability has demonstrated the intricate differences that exist in the regulatory environment for unlawful content and the enforcement options available against intermediaries.

First, in certain content areas, the substantive, normative law provisions differ between Member States (hate speech, defamation, copyright). Some national laws incorporate specific intermediary consideration into their frameworks, as was demonstrated for the 1881 French Press Law, or the 2013 UK Defamation Act. This affects the way the content management practices and the duties of intermediaries are being evaluated on a purely normative way. A prime example here are the different degrees to which certain content is seen as manifestly illegal. These kinds of differences could, arguably, be ironed out by a further increase in competencies at EU level, through further harmonisation of hate speech or even defamation laws,[1644] or copyright exemptions. The enlargement of EU competencies is in itself, however, a highly contentious policy issue. It is not sure whether the usual justifications provided by the internal market and fundamental rights will achieve such harmonisation in the face of pronounced national interests and national competencies, as for example for media law[1645] or national security.

Secondly, the enforcement regimes of each content area vary significantly. In the public law dominated areas of terrorist content and product regulation, there is a marked engagement of law enforcement and surveillance authorities with intermediaries. In private law areas concerning personality and economic rights, enforcement happens mainly through courts.

Thirdly, the free-standing national secondary intermediary liability rules, principles and legal traditions vary across Member States. They also interact to different degrees with sector specific laws.[1646]

Fourthly, the relatively plain and general ECD intermediary liability framework is superimposed on the rich national secondary liability rules and sectoral law. This has a led to disparate interpretations and applications of these rules across the EU. The ECD may be used as an additional

---

1644 Savin (n 384) 142.

1645 Cornils (n 481) 80–81.

1646 For example, as could be seen in the area of defamation and hate speech, the French Press Law excludes the application of the secondary liability provisions of the Code Civil.

option to existing national liability provisions, in conjunction with them[1647] or by being replaced almost exclusively with local secondary liability concepts. The limited arsenal of secondary liability and intermediary sanctions offered through EU laws (ECD, IPRED and the Infosoc Directive)[1648] is eclipsed by a rich repertoire at Member State level.

Fifth, the minimum harmonisation approach of the ECD also means that some Member States have developed their own NTD procedures through law or self-regulatory arrangements, while others have not regulated this at all. This in turn has had an influence on the definition of the knowledge standard by jurisdiction and by content area, as well as on procedural obligations.

All this makes each content sector a distinct multi-level regulatory space, with particular enforcement practices. This landscape is complicated by the fact that within these vertical regulatory spaces, enforcement approaches vary on a horizontal level between countries.

Lawmakers at both EU and national level from various regulatory areas have reacted differently to harmful content management practices of online platforms. Initial attempts to foster self–regulatory initiatives through e.g. codes of conduct, as provided for by the ECD[1649] have been partially followed up by more decisive policy action in selected areas. The EU's regulatory choice of new legislative initiatives is, however, different. In the area of copyright, the DSM has now removed OCSSPs from the scope of the ECD by making them primarily liable for unauthorised content. To protect against direct infringement, OCSSPs will need to strike licensing agreements with rightsholders or show that they have made best efforts to prevent any unauthorised acts. The resulting obligations are to be put in place through self-regulatory arrangements between intermediaries and the rightsholder industry. The AVMSD deploys a slightly different model in the fight against hate speech and content harmful for minors on VSPs. Secondary liability would ensue where VSPs fail to adequately deploy a set of defined preventive measures. The regulatory setup is rounded off by charging ERGA with a coordinating function, which is a first step in the direction of a co-regulatory structure. The proposed anti-terrorism regulation follows a more traditional, rule-making approach by imposing fixed removal deadlines and potential obligations for proactive removal and identification of content. In the area of product and food safety, EU legis-

1647 Oster (n 816); Benabou (n 334).
1648 Leistner (n 336) 78–89.
1649 Directive 2000/31 (ECD) Article 16.

lative initiatives have so far not allocated enhanced responsibilities to online platforms, except for an obligation to cooperate with MSAs in specific cases concerning safety risks of non-food products. The picture is completed by national initiatives such as the *NetzDG* or the now defunct *Loi Avia*, which have pursued either self- or co-regulatory solutions.

2. Summary: Common trends in sectoral online intermediary liabiliy

> *"The problem with many current cyberlaw texts is that questions of intermediary liability are scattered throughout chapters focusing on specific kinds of tortious liability–copyright, trademark, defamation, etc. This organization tends to discourage a focus on the central question involving the rights and obligations of intermediaries across discrete subject matter areas."*[1650]

The analysis in this chapter has exposed a heterogeneric enforcement landscape across different content sectors, which currently seems to develop even further apart. The abandonment of horizontal principles of online intermediary responsibility could seem a plausible solution for accommodating pragmatic, effective and flexible content specific solutions. It is certainly important to respect differences in normative aspects, regulatory specificities and technical details across content sectors. However, this chapter also demonstrated that today's Web 2.0 platforms display essential commonalties that call for horizontal principles of unlawful content prevention on online platforms.

First, in all areas covered, there is a marked push of damaged parties, legislators and enforcers to allocate enhanced responsibilities on intermediaries that are commensurate with their business models in general, and their content management practices in particular. The driver for this appears to be less the degree of manifest illegality of content, but rather more the deep involvement and integration of these platforms in the act of information intermediation. Apart from a push towards enhanced secondary liabilities, this has also led to forays into the area of primary liability allocation, e.g. in copyright. In that context, the distinction between neutral and active intermediaries is by now hopelessly outdated and should be replaced by less rigid criteria that are applied horizontally. Secondly, many of the large integrated platforms straddle different legal content areas, be they copyright, hate speech, trademarks or unsafe products. Common horizontal responsibility

1650 Lipton (n 287) 1346.

principles make therefore for more legal certainty for both users and platform operators themselves. Third, online platforms work according to similar underlying business models and architectural design decisions. They are focussed on exploiting user data, or behavioural surpluses. Content moderation is primarily based on commercial interests.[1651] Fourthly, at least the large, dominating platforms have expanded their automated content management practices to create systems that detect and remove unlawful content. They enforce mainly along their own private content policies, with a secondary regard for the applicable laws. Whether it concerns terrorist speech, copyright violations or unsafe product identification, the procedures and criteria that govern these decisions are mainly driven by commercial objectives. However, they remain largely inaccessible to those parties most concerned by their application. These private content management practices have a significant impact on fundamental rights, such as privacy or human dignity, freedom of expression, economic rights, or public health and safety. The ubiquity and power of online platforms on the internet means that these private norms have become quasi law, and intermediaries akin to parallel states,[1652] that override the public interest criteria formulated and enforced by democratically elected governments. This tendency is observed in each of the content sectors covered above.

This all calls for more wide-reaching responsibility criteria and systemic harm prevention approaches that go beyond content type specific considerations.[1653] A horizontal, principles-based framework would allow for addressing these commonalities in a holistic way by also exploiting synergies between the different, already existing approaches. Finally, such a system would facilitate an easier interlinkage with other legal domains that have become crucial when addressing critical issues of online platform power, such as competition law, data protection, consumer law or IT security.[1654]

1651 Zuboff (n 5). Sarah Jeong, *The Internet of Garbage* (1.5, Vox Media, Inc 2018) Ln 1084 - 1384.

1652 Tambini and Moore (n 232) 406; Natali Helberger, 'Challenging Diversity - Social Media Platforms and a New Conception of Media Diversity' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 167.

1653 Taddeo and Floridi (n 120) 1598; Burk (n 295) 452. Lipton (n 23) 155–157.

1654 Tambini and Moore (n 232) 399–406; Peggy Valcke, Inge Graef and Damian Clifford, 'IFairness – Constructing Fairness in IT (and Other Areas of) Law through Intra- and Interdisciplinarity' (2018) 34 Computer Law & Security Review 707, 710–711. Vassilis Hatzopoulos, 'Vers un cadre de la régulation des plateformes?' (2019) XXXIII Revue internationale de droit économique 399, 414.