Chapter 3 - Intermediaries and unlawful content – challenges in internet regulation

A. The subject matter of internet governance

Regulation of the internet has traditionally focussed on two major aspects: infrastructure and content.[266] Both shall be briefly discussed below.

1. Infrastructure

Consideration of internet regulation or internet governance goes back to the time when the internet still existed as a publicly funded, closed research project. Its release into the market during the 1990s happened out of a deeper appreciation, mainly by US public and academic stakeholders, that the internet could only fulfil its potential through commercial investment into physical infrastructure and exposure to creative market forces.[267]

As explained above, it is a unique design feature of the internet that it integrates and runs almost seamlessly on all underlying physical communication networks, as longs as those networks adopt the different layers of protocols. The term 'infrastructure' of the internet therefore refers to several features: first, there are the physical assets such as data centres, communication lines, exchange points or routers. In addition, this includes less tangible things such as technical standards, software programs or processes, e.g. the internet's protocols, communications standards, data storage or memory, and databases. Finally, end devices, e.g. mobile phones or PCs,

266 Scholte (n 23) 165; Panos Constantinides, Ola Henfridsson and Geoffrey G Parker, 'Introduction—Platforms and Infrastructures in the Digital Age' (2018) 29 Information Systems Research 381; Rolf H Weber, *Shaping Internet Governance: Regulatory Challenges* (Springer Berlin Heidelberg 2010) 4–5. Francesca Musiani, 'Alternative Technologies as Alternative Institutions: The Case of the Domain Name System' in Derrick L Cogburn and others (eds), *Turn to Infrastructure in Internet Governance* (Springer Nature 2016).

267 Castells (n 3) 69; Garcia (n 97) 541–543.

have become an ever more important element of the digital infrastructure.[268]

Given this heterogeneity, one of the first concerns was therefore to ensure that the technical interoperability of the internet's digital infrastructure remained intact once it was commercialised. A technical governance structure was therefore set up by the US Government over the 1980s, while the internet was still a publicly funded undertaking. The regulatory arrangement reflected the US Government's credo of self-regulation.[269] Institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) or the Internet Society Internet (ISOC) are all private, not for profit organisations that control and decide on matters relating to the internet's address system or the technical standards behind protocols and data communication.

These organisations were set up in a way that allowed for participation by worldwide internet communities and decisions being made on a consensual basis. The role of states is usually limited to representative or advisory functions along with other interest and user groups, such as civil society or technical bodies.[270] For example, most states are represented on the Government Advisory Committee of ICANN, while a number of international organisations act as observers. Overall, there is a strong focus on broad, multi-stakeholder representation and technical expertise.[271] This system initially also coincided with the early internet pioneers' vision of an open and largely auto-regulated cyberspace.

---

268 Constantinides, Henfridsson and Parker (n 265) 381. This digital infrastructure is different to what is sometimes referred to as private infrastructure or platform control over internet infrastructure. That term relates to a platform's technology to manage content hosted on its servers. (See: Robert Gorwa, 'The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content' [2019] Internet Policy Review Fn 1. or Lina M Khan, 'Amazon—An Infrastructure Service and Its Challenge to Current Antitrust Law' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018). and Francesca Musiani and Laura Denardis, 'Governance by Infrastructure' in Laura Denardis and others (eds), *Turn to Infrastructure in Internet Governance* (Springer Nature 2016) 5.

269 Collins (n 116) 52. Reidenberg (n 90) 921.

270 Weber (n 265) 39–72.

271 For example: 'ICANN Organizational Chart - ICANN' <https://www.icann.org/resources/pages/chart-2012-02-11-en> accessed 8 August 2019. '2016 W3C Internal Reorganization' <https://www.w3.org/2016/08/2016-reorg.html> accessed 8 August 2019.

These governance arrangements have been seen as an early manifestation of a move away from hierarchical regulation to network governance structures, in a bid to adapt to increasingly complex and globalised contemporary society.[272]

Nevertheless, the debate over the control of the infrastructure has also become more political as the economic and public role of the internet increased. The fact that the US was the only nation state that until recently exercised direct control over ICANN, the key organisation when it comes to maintaining the technical infrastructure of the internet, played a major part in this conflict.

The US relinquished its control over ICANN in 2016. It initiated a new governance structure which strengthened industry and civil society sector control and aimed to exclude control of any other state over ICANN. Some commentators have inferred that this change was helped by the fact that the world's leading online intermediaries, which facilitate, some might say control, access to content and growing parts of the digital infrastructure, are US corporations, that, at least up to 2016, shared wider US Government policy concerns.[273]

There is no space here to sketch the political power struggles that have taken place at an international level over the administration over the internet's root servers and the domain name system.[274] However, these developments are also seen as a consequence of the debate over content regulation spilling over into the area of infrastructure governance.[275]

As large internet platforms control significant spheres of the internet's content, leverage over the internet's neutral, content agnostic digital infrastructure is seen as an alternative means to influence or affirm power over the internet and its content flows. This is a specific feature of the open and modular structure of the internet. Content flows can be influenced by con-

---

272 Rolf H Weber', 'Future Design of Cyberspace Law' (2012) 5 Journal of Politics and Law 15, 5; Collins (n 116) 52.

273 Manuel Becker, 'When Public Principals Give up Control over Private Agents: The New Independence of ICANN in Internet Governance' [2019] Regulation & Governance rego.12250.

274 Nanette S Levinson and Meryem Marzowski, 'International Organizations and Global Internet Governance: Interorganizational Architecture' in Derrick L Cogburn and others (eds), *Turn to Infrastructure in Internet Governance* (Springer Nature 2016).

275 See for example: Kenneth Merrill, 'Domains of Control: Governance of and by the Domain Name System' in Derrick L Cogburn and others (eds), *Turn to Infrastructure in Internet Governance* (Springer Nature 2016).

trols over the digital infrastructure: the address system (disabling domains or IP addresses), via labelling/stamping of content at the logical layer (securing or identifying content through data packet header modification and encryption) or by physically controlling exchange points where traffic passes from one network provider or communication system to another.[276] For example, digital infrastructure governance organisations, like ICANN or downstream domain registration services, are increasingly called upon when it comes to fighting unlawful content.[277] By contrast, in other content systems, such as telecoms and television, control can be exerted by keeping networks closed.[278]

2. Content regulation = intermediary regulation?

In its very early days, internet regulation or governance was mainly concerned with digital infrastructure. This changed quickly as connectivity grew and diverse content started to circulate on the commercial web. Since the mid-1990s, cyber law researchers had already remarked on the potential of the internet to attract massive amounts of illegal content and activity and they debated on how to address this challenge.

Johnson & Post represented the cyber libertarian view of a distinct, autoregulated cyberspace in which users and engineers enforced agreed rules through systems operators, user conduct and public education.[279] *Lessig* contrasted this view by predicting that regulators would extend their influence towards the internet and its architecture. They would regulate web access to content by creating boundaries or zones through coding: an example used was the creation of technical protections of copyrighted material. Commercialisation of the web relies on property, *Lessig* argued. Property, in turn, relies on boundaries.[280]

---

276 Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011) 22–25.

277 Annemarie Bridy, 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation.(Internet Corporation for Assigned Names and Numbers)' (2017) 74., *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta - C-521/17* [2018] EU:C:2018:639 (CJEU).

278 Marsden, *Internet Co-Regulation* (n 275) 23. This is somewhat undermined by the convergence of these systems with the internet, i.e. Voice over IP (VoIP)

279 Johnson and Post (n 87).

280 Lessig, 'The Zones of Cyberspace' (n 92) 1407–1410.

Without meaning to pre-empt, it should be mentioned that by the early 2000s illegal content on the internet had become a massive problem for policy makers.[281] This was exacerbated by the global spread of the internet, the first sprouts of Web 2.0 activity and the intermediation of content through platforms.[282]

Regulation of content that was facilitated by intermediaries moved gradually to the centre stage of internet regulation and has remained there since.[283] Given the rise of power of intermediaries, online platforms in particular, and the continued prominence of the problem of unlawful information, content regulation has become enriched with other areas of problematic platform dominance, such as competition and privacy law. In line with these more holistic concerns over the unfettered power of online platforms there has been a tendency to draw infrastructure regulation back into this equation.[284] Some commentators have advocated for overcoming the distinction between content and infrastructure regulation.[285] This should be kept in mind in the sectoral analysis of intermediary liability and of content regulation.

It has been a characteristic of content regulation since the internet's beginning that states were seeking to assert their jurisdiction more aggressively than in the area of infrastructure.[286] Unlawful content is defined and regulated differently across jurisdictions, be it hate speech, defamation, intellectual property infringments or terrorist material. The public policy objectives of states may be directly impacted when unlawful material is being accessed and shared by their populations. But the global and distributed nature of the internet's content and infrastructure mean that national en-

281 Christopher T Marsden, 'Co- and Self-Regulation in European Media and Internet Sectors: The Results of Oxford University's Study Www.Selfregulation.Info', *Self-regulation, Co-regulation, State Regulation* (OSCE 2004) 95 https://www.osce.org/fom/13844?download=true, or Uta Kohl, 'The Rise and Rise of Online Intermediaries in the Governance of the Internet and beyond – Connectivity Intermediaries' (2012) 26 International Review of Law, Computers & Technology 185, 204–205.

282 Francisco Javier Cabrera Blázquez, 'User-Generated Content Services and Copyright' (2008) 5 iris plus 1.

283 See for example: Hans J Kleinsteuber, 'The Internet between Regulation and Governance', *Self-regulation, Co-regulation, State Regulation* (OSCE 2004) <https://www.osce.org/fom/13844?download=true>. Kleinsteuber mentions internet regulation exclusively in the context of regulating content.

284 Musiani and Denardis (n 267) 5–6.

285 William J. Drake in: Weber (n 265) 6–7.

286 Scholte (n 23) 165.

forcement of content regulation is regularly frustrated. The problem is exacerbated as the internet becomes omnipresent in peoples' lives and, thanks to online platforms, indispensable throughout many parts of the world.

It can therefore safely be presupposed that, at least since the rise of the Web 2.0, internet regulation refers to a large extent to the content management practices of internet intermediaries.[287] These intermediaries are usually not in the first line of responsibility for the creation of unlawful content by their users. Without them, however, worldwide availability of content and its spread would be significantly hampered.

Given this indispensable role of intermediaries for the availability of content some commentators have come to define intermediary regulation as the very substance of cyberlaw today.[288] *Lessig's* assertion of the role of code as a quasi-regulator of user behaviour may still be valid. But this does not mean that law, cyberlaw specifically, is not needed to define and sanction unacceptable and unlawful user behaviour or content.[289]

As this work addresses the responsibilities of platforms *vis-à-vis* unlawful content (in the EU), it is necessary to review and analyse past regulatory efforts made in this area.

B. The emergence of internet intermediary liability

In the following, a brief overview will be given over the emergence of the internet intermediary regimes in the EU, the US and a number of other jurisdictions. Before this, it is appropriate to describe some general consideration of the role of intermediaries and their liabilities in the law. The different justifications for allocating liabilities to intermediaries and the varying types of liability that have developed under different legal systems are important elements that influence the regulation of these actors today.

287 Wagner, *Global Free Expression - Governing the Boundaries of Internet Content* (n 136) 104–118.

288 Jacqueline D Lipton, 'Law of the Intermediated Information Exchange' (2012) 64 Florida Law Review 33, 1338.

289 ibid 1342.

1. Justifications for internet intermediary liability in law

I. Moral justifications

Intermediaries, as entities that facilitate commercial and private interactions by third parties, have been existing since well before the internet. Classifieds newspapers, market halls that rent out stalls to traders, or financial service brokers are just some examples of such intermediaries. The discussion on internet intermediary liability is also informed by the doctrinal literature and case law from this pre-internet era. The moral arguments are strongly influenced by utilitarian thinking that can be traced back to *Mills:*

> "*To make any one answerable for doing evil to others, is the rule; to make him answerable for not preventing evil, is, comparatively speaking, the exception. Yet there are many cases clear enough and grave enough to justify that exception. In all things which regard the external relations of the individual, he is de jure amenable to those whose interests are concerned, and if need be, to society as their protector.*"[290]

According to *Mills* the "answerability" or liability of the agent arises out of a failure to act or prevent harm that is caused by one party to another. According to the utilitarian argument an agent would have a duty to act, even where it is against its own interests, when the harm caused leads to a net loss in happiness to society.[291]

On the other hand, following the *Kantian* logic of duty ethics, an intervening agent or intermediary would have a moral duty to act in a virtuous way, i.e. a way that is in line with its moral duties as an actor of society.[292] Under that approach an intermediary would be less likely to focus on the consequences of the harmful acts performed through them but rather be required to abstain from *any* harmful or non-virtuous behaviour.

Lawmakers have the opportunity to impose duties and responsibilities on intermediaries following these moral considerations. According to *Vedder*, content responsibilities imposed on internet intermediaries may be prospective or retrospective.[293] Prospective (moral) responsibilities would

290 John Stuart Mill, *On Liberty and Other Essays* (Digireads (2010 edition) 1859) 11.
291 ibid 84.
292 Thomas H Koenig and Michael Rustad, *Global Information Technologies: Ethics and the Law* (West Academic 2018) 67–68.
293 Anton Vedder, 'Accountability of Internet Access and Service Providers – Strict Liability Entering Ethics?' (2001) 3 Ethics and Information Technology 67, 68. Helberger, Pierson and Poell (n 68) 2.

impose duties and obligations on intermediaries aimed at preventing harm. Prospective responsibilities would be a precondition for being able to impose retrospective responsibilities. Retrospective, backward-looking or historic responsibilities would allocate blame to past actions of intermediaries.[294]

At least as regards internet intermediaries, prospective and retrospective responsibilities are reconcilable with utilitarian moral approaches.[295] In the former case, the intermediary's responsibilities are adjusted to their "ability to acquire, comprehend, and act upon socially relevant information."[296] This requires an impact estimation and would result in preventive responsibilities that create the largest net welfare or happiness. Retrospective considerations under a utilitarian scenario would adjust responsibilities to the negative impacts or harms caused, by for example attributing redemptive, retributive measures or by imposing deterrent measures to prevent similar harms in the future.[297]

Deontological approaches try to ascertain the agent's moral duties. In a forward-looking scenario, society would form a consensus view on the wider role of the agent, e.g. the expected moral behaviour of internet intermediaries, and define legal responsibility that correspond to that role.[298] *Yeung et. al.* refers to this as the 'role responsibility' when talking about ethics in artificial intelligence systems and robotics systems.[299] By contrast, retrospective responsibilities allow for verification of whether an intermediary has complied with the moral duties imposed on them in the first place (prospectively). This review would centre on the moral integrity of the agent and allows for balanced and contextual analysis.[300]

---

294 Helberger, Pierson and Poell (n 68) 11; Karen Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), 'Responsibility and AI' (2019) Council of Europe study DGI(2019)05 48 <https://edoc.coe.int/en/artificial-intelligence/8026-responsibility-and-ai.html> accessed 11 November 2020.

295 Vedder (n 292) 68, 71–73.

296 Dan L Burk, 'Toward an Epistemology of ISP Secondary Liability' (2011) 24 Philosophy & Technology 437, 443.

297 Vedder (n 292) 69.

298 Derek E Bambauer, 'From Platforms to Springboards' (2018) 2 Georgetown Law Technology Review 15, 430.

299 Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (n 293) 51–53.

300 Vedder (n 292) 69–70.

The concept of prospective responsibility becomes important in the context of novel technologies and architectures deployed by digital platforms and the uncertainty over the harms they may cause. The debate centres on to what extent harms caused by platforms' own business models and systems were reasonably foreseeable. Meanwhile, retrospective, or historic responsibility would include measures that are taken *ex-post* in order to address and correct harms caused.[301]

II. Economic justifications

According to the cheapest cost avoider theory developed by *Coase* and *Calabresi*[302] liability should be allocated to the economic actor that is able to avoid a wrongdoing at the lowest cost. This cost comprises the economic investment of an entity into the prevention of unlawful activity as well as the external social costs and benefits of that intervention to society. Under this theory "a liability regime is optimal when it creates incentives to maximise the value of risky activities net of accident and precaution costs."[303] Meanwhile there is no unified view on whether a standard of strict, or primary liability, or a fault-based (secondary) liability standard would create the optimal incentives for a cheapest cost avoider.[304]

While originally not focussed on transactions that involve multiple parties, more recent research has looked at the problem of applying the cheapest cost avoider principle to multiple actor scenarios.[305] Intermediaries, or third parties, are drawn into this equation when they occupy positions that are central or indispensable for the activities in question. In this case they

---

301 Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (n 293) 59–68.

302 RH Coase, 'The Problem of Social Cost' (1960) 3 The Journal of Law and Economics 1; Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis* (Yale University Press 1970).

303 Emanuela Carbonara, Alice Guerra and Francesco Parisi, 'Sharing Residual Liability: The Cheapest Cost Avoider Revisited' (2016) 45 The Journal of Legal Studies 173, 173.

304 Andrew F Tuch, 'Multiple Gatekeepers' (2010) 96 Virginia Law Review 1583, 1622.

305 Assaf Hamdani, 'Gatekeeper Liability' (2003) 77 Southern California Law Review 53; Tuch (n 303). In addition, the different components of the cheapest cost avoider, such as risk and the value of activities are also being "unpacked" in Carbonara, Guerra and Parisi (n 302) 173–201.

are also referred to as gatekeepers. Broadly speaking, gatekeepers are "… parties who sell a product or provide a service that is necessary for clients wishing to enter a particular market or engage in certain activities."[306]

Under the cheapest cost avoider principle an intermediary would be allocated with legal responsibilities and subsequent liabilities, if, in addition to their gatekeeping, role they have the capabilities to detect and prevent wrongdoings of their clients, or other contractual parties, at a reasonable cost.[307] This presupposes a certain element of control and knowledge of the gatekeeper over the activities of its client.

While there is little doubt today over the utility of enrolling gatekeepers in the fight against unlawful activity, there is much less clarity and agreement over the most efficient and adequate means of how to get it right. This has much to do with the fact that gatekeepers often possess superior knowledge over their clients' activities compared to regulators and have better technical and more effective means to gain such knowledge, evaluate the corresponding risks, and hand out sanctions.

The financial services sector, with its complex technical network of interdependent service intermediaries, such as accounting firms, insurers, rating agencies or auditors, has been an area of predilection for research in this area. This research has been spurred further by the *Enron* accounting scandals and the 2007 subprime financial crisis.[308] However, internet intermediaries have also moved into the focus of economic law theory on gatekeeper regulation, given their essential function as access providers to information and communication.[309]

Economic law theory is still in want of models to determine what kind of liabilities (strict, negligence- or knowledge based) are most effective in a given multiple-gatekeeper context. In addition, the cheapest cost avoider theory is also criticised for its inflexibility. The focus on identifying and ascribing liability to a cheapest cost avoider tends to overlook the opportunities that can be gained from establishing processes and mechanisms that reduce costs.[310] A collaboration of gatekeepers and economic actors and a split of legal responsibilities could result in such a reduction of costs. *Helman and Parchomovsky* and *Helberger et al* have explored this concept of co-

306 Assaf Hamdani (n 304) 58.
307 ibid 99.
308 Stavros Gadinis and Colby Mangels, 'Collaborative Gatekeepers' (2016) 73 Wash. & Lee L. Rev. 797, 812–815. Assaf Hamdani (n 304).
309 Assaf Hamdani (n 304) 99–108.
310 Lital Helman and Gideon Parchomovsky, 'The Best Available Technology Standard' [2011] Columbia Law Review 1194, 1212–1213.

operative responsibility or risk sharing in the area of content regulation and online intermediaries.[311] This involvement of multiple actors, however, is bound to add to the complexity that the cheapest cost avoider principle and economic regulation pose already for much more straightforward dual-actor scenarios. In addition, the unique characteristics of online platform markets have thrown further doubt on the application of economic regulation theories of risk-modelling and cost-benefit analysis to cyberspace.[312]

Courts and regulators in the US and the EU have nevertheless taken up the cheapest cost avoider principle as a justification for allocating liabilities to intermediaries, albeit not always in a consistent way.[313]

2. Primary and secondary liability

There are two possibilities of holding an intermediary liable for unlawful or harmful acts by third parties: primary or strict liability, and secondary liability.

The kind of liability that can be ascribed to intermediaries depends on the type of action or non-action (including non-performed duties and obligations) that justify the attribution of harm. A clear causal relationship between action/omission and the harm caused are a pre-condition for finding liability.[314] *Vedder* argues that this causal relationship is a characteristic of retrospective responsibility and therefore not necessary in finding liability for breach of a prospective duty.[315] An example here would be failure of an agent to comply with a statutorily imposed duty of care or compliance obligation in the absence of actual harm or damage caused by that shortcoming.

311 Helman and Parchomovsky (n 309); Helberger, Pierson and Poell (n 68).

312 Niva Elkin-Koren and Eli M Salzberger, 'Law and Economics in Cyberspace' (1999) 19 International Review of Law and Economics 553, 577–580; Cohen (n 19).

313 Graeme B Dinwoodie, 'Secondary Liability for Online Trademark Infringement: The International Landscape' (2014) 37 Columbia Journal of Law & the Arts 463, 499–501.

314 Augustin Waisman and Martin Hevia, 'Theoretical Foundations of Search Engine Liability' (2011) 42 International Review of Intellectual Property and Competition Law 785, 791.

315 Vedder (n 292) 68.

In many cases the borders between primary and secondary liability are fluent and far from clear-cut.[316] Consequently, findings of primary or secondary liability depend on the type of involvement, or the degree of relative responsibility of the actor in the causal chain of events which led to the breach or damage.

It is worth noting that the concept of (intermediary) liability discussed here does not mean contractual liability. Strict or primary liability refers generally to the extent to which an intermediary can be held responsible for the action of others, regardless of whether contracts are in existence or not.[317]

I. Primary liability for intermediaries

Primary or strict liability lies usually with the manufacturer, publisher or creator of a product, service or piece of work. However, in most legal systems this may be extended to other parties, such as intermediaries, if they introduce an additional risk into the issue at stake.[318]

For example, in EU product safety law, distributors have normally indirect, or secondary due care obligations to help ensure that only safe products are supplied to consumers.[319] Once, however, their activities directly affect the properties of a product, such as manipulation, repackaging or in-

316 Kohl (n 280) 191. Thibault Verbiest and others, 'Study on the Liability of Internet Intermediaries, Markt 2006/09/E' 54.

317 Without pre-empting the discussions made in this and the next Chapter, this is confirmed by the intermediary liability regime imposed by the ECD (Articles 12 – 15). It stipulates general liability conditions for the actions concerning third parties. However, failure to comply with these conditions may then trigger all sorts of liabilities, including contractual, administrational, tortuous, penal or civil liabilities. Patrick Van Eecke and Maarten Truyens, 'Legal Analysis of a Single Market for the Information Society (SMART 2007/0037) - Part 6 - Liability of Online Intermediaries' (European Commission 2011) 8–9 <https://ec.europa.eu/digital-single-market/en/news/legal-analysis-single-market-information-society-smart-20070037> accessed 4 February 2020; Etienne Montero, 'La responsabilité des prestataires intermédiaires sur les réseaux' [2001] Le commerce électronique européen sur les rails? : Analyse et propositions de mise en oeuvre de la directive sur le commerce électronique 273, 291.

318 Waisman and Hevia (n 313) 791.

319 Directive 2001/95/EC of 3 December 2001 on general product safety (OJ L 11) Article 5 (2).

appropriate handling, they become primarily liable for the safety of the product.[320]

In EU copyright law primary liability normally lies with the person who reproduces protected works without the permission of rightsholders.[321] However, primary liability may also lie with other parties that communicate and make available to the public protected works without seeking necessary permissions.[322] In *The Pirate Bay* ruling the CJEU found that an online platform, which merely indexed entertainment content available for download elsewhere, performed an act of communication to the public. It was therefore directly liable for facilitating the unauthorised peer-to-peer exchange of copyrighted protected works.[323]

The recently passed EU Copyright in the Digital Single Market Directive (DSMD) introduces direct copyright liability on online content-sharing platforms.[324] According to the EU legislator, the additional risk introduced by these intermediaries lies in the fact that: 1) they provide access to large amounts of copyright-protected content; 2) legal uncertainty exists as to whether these platforms perform copyright-relevant acts.[325]

II. Secondary liability

Secondary liability takes account of the fact that a party, although it had no direct part in an action, may still have had a degree of involvement that justifies the impositions of obligations to prevent or end unlawful activities.[326] Failure to fulfil these duties or obligations would then result in liabilities.

---

320 ibid Article 2 (f).

321 Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society 2001 (OJ L 167, 2262001) Article 2.

322 ibid Article 3.

323 *Stichting Brein II* (n 214) paras 38–43.

324 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) 2019 (OJ L 130) Article 17. The term content –sharing platforms will be applicable to most UGC or social media platforms.

325 ibid Recital 61.

326 'What Is SECONDARY LIABILITY? Definition of SECONDARY LIABILITY (Black's Law Dictionary)' <https://thelawdictionary.org/secondary-liability/> accessed 13 August 2019.

a. Common law

In common law jurisdictions the concept of secondary liability has been further developed by courts, resulting in the distinction between vicarious and contributory liability.[327]

In vicarious liability an entity is held responsible for the infringing acts of agents over which it exerts control. Apart from the typical liability of the *respondeat superior* for the actions of its employees, this concept has been extended towards other principal-agency relationships in a commercial context.[328] Vicarious liability usually results in courts finding a faulted party strictly liable, regardless of whether the act was performed intentionally or not.

Contributory liability, by contrast, takes knowledge of the infringing activity as a yardstick. The contribution to infringement may happen by participation or by supplying the means to the unlawful activity. Typical cases here relate to the supplying of technology, capacity or advertisement for unlawful acts.[329] Where a party was found to have had knowledge over the unlawful activity or could have been expected to know about it as a reasonably responsible actor, this results in indirect liability and therefore a lesser degree of punishment compared to strict or primary liability. Likewise, courts may look at passive and active knowledge or negligence when determining contributory liability.[330]

Both vicarious and contributory liability

> *"…endorse a form of enterprise liability as a vehicle for creating obligations to police third-party behavior. The risk of liability is such that nearly all (lawful) services are compelled to shoulder a regulatory burden, and the ef-*

327 Alfred C Yen, 'Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment' 88 The Georgetown Law Journal 63, 1872.

328 For example, dance hall operators for the unauthorised performance of music by music bands, or landowners for the unlawful activity of businesses being invited on their premises; more detail in: Burk (n 295) 439–440.

329 ibid 440.

330 Richard W Wright, 'Allocating Liability Among Multiple Responsible Causes: A Principled Defense of Joint and Several Liability for Actual Harm and Risk Exposure' 21 UC Davis Law Review 1141, 1159.

fect perceived by the consumer is a uniform marketplace where policing occurs."[331]

b. Civil law jurisdictions

In the EU, where most countries rely on a civil law legal system, the landscape of secondary liability rules is more disparate. The interplay between differing national secondary liability provisions and their application by courts on the one hand, and EU law on the other, result in a heterogeneous landscape regarding liabilities and remedies.[332] As an illustration, the secondary liability rules in three EU Member States will be briefly mentioned below.

In France, contributory liability is first regulated on a general level by the *Code Civil*.[333] Articles 1240 – 1241 impose civil liability in cases where harm is inflicted and where negligence has caused damage. Both articles are fault based and allow for the allocation of a wide range of civil remedies. The *Code Civil* imposes an intentionally wide obligation for compensation. This follows the civil law tradition of broadly protecting the individual rights of persons on the one hand, while ensuring adaptability of the law to changing circumstances in society on the other.[334] Apart from that, contributory liability can also be established through a duty to act established by statute.[335]

In Germany, contributory liability is expressed by the concept of "*Störerhaftung*" ("interferer liability") laid down in the German civil code

331 Matthew Schruers, 'Copyright, Intermediaries, and Architecture' in Francesca Musiani and others (eds), *Turn to Infrastructure in Internet Governance* (Springer Nature 2016) 110.

332 Dinwoodie (n 312) 485.

333 Code civil - Articles 1240 & 1241 (Code civil). Articles 1382 and 1383 prior to the 2016 reform of the Code Civil.

334 Karen Eltis, 'Can the Reasonable Person Still Be "Highly Offended" - An Invitation to Consider the Civil Law Tradition's Personality Rights-Based Approach to Tort Privacy' [2008] University of Ottawa Law & Technology Journal 199, 212–213.

335 For a more detailed description: Martin Vranken, 'Duty to Rescue in Civil Law and Common Law: Les Extremes Se Touchent' (1998) 47 International and Comparative Law Quarterly 934, 937–941. and Valérie Laure Benabou, 'Quelle(s) responsabilité(s) des intermédiaires techniques sur Internet?' (2006) 61 Annales des télécommunications 865.

(BGB).[336] This implies a wilful, causal contribution to the infringing act and the possibility of preventing the violation through a reasonable duty of care. It results in courts imposing injunctions, but usually not damages.[337] Outside of this, statutes may, like in France, provide for specific duties of care, subsequent tort liabilities and remedies (including damages). In Germany, as in other jurisdictions, the distinction between secondary, interferer style liability, and direct liability caused by abetting or contributing to an infringing act has become increasingly difficult to make.[338] This is due to the complex and often opaque involvement of online platforms in the information intermediation process. The distinction is made even more difficult by the fact that both liability concepts usually presuppose the violation of certain duties of care.[339]

Italian law applies secondary liability mainly in the form of vicarious liability following the *respondeat superior* doctrine. By contrast, contributory liability is less clearly expressed and would mainly be applied through the principles of joint or several liability (in the Italian Civil Code).[340]

Some authors have contrasted a broad approach towards contributory liability in civil law with a more rigid approach in common law. In the latter, they argue, a legal duty of care has never existed *per se*.[341] Precedence-based common law resulted in the development of categorised torts, each defined by specific criteria, to be verified by tests applied in courts.[342]

It is impossible to give a comprehensive overview of secondary liability rules across all Member States here. However, it can be safely assumed that standards of secondary liability that apply concepts of negligence through failure of applying a reasonable duty of care are in place throughout the

336 Bürgerliches Gesetzbuch Article 1004.

337 M Leistner, 'Structural Aspects of Secondary (Provider) Liability in Europe' (2014) 9 Journal of Intellectual Property Law & Practice 75, 79.

338 Thomas Hoeren and Viola Bensinger (eds), *Haftung Im Internet: Die Neue Rechtslage* (De Gruyter 2014) 395–396.

339 ibid 395.

340 Elisa Bertolini, Vincenzo Franceschelli and Oreste Pollicino, 'Analysis of ISP Regulation under Italian Law' in Graeme B. Dinwoodie (ed), *Secondary liability of internet service providers* (Springer Berlin Heidelberg 2017) 141–142. Codice Civile 1942 Article 2055.

341 Vranken (n 334) 935.

342 John DR Craig, 'Invasion of Privacy and Charter Values: The Common-Law Tort Awakens' (1997) 42 McGill Law journal 355, 363; Eltis (n 333).

EU Member States and other jurisdictions, albeit in different forms and with various types of sanctions.[343]

These considerations shall be kept in mind during the review of online intermediary case law in this and the next Chapter, and when discussing policy reactions and proposals for intermediary regulation.

As a general rule, secondary liability therefore hinges on two elements: 1) control of the agent over the other parties' activities and 2) knowledge of potential or actual breaches of law or injuries to other parties. In both cases, liability would be caused by failure to comply with obligations that could be reasonably expected from the agent given its degree of control and knowledge.[344] The active or passive involvement of the intermediary may be an additional vector to indicate the degree of liability. Control, knowledge, and active versus passive engagement are also the most controversial issues in the current debate over the duties and liabilities of online platforms for unlawful content, as will be explained later.

3. Early case law on internet intermediaries

In the 1990s, the internet and internet intermediaries were a new, technologically complex and rapidly expanding phenomenon. Unlawful content on the internet related mainly to defamation, hate speech or illegal pornographic material (including child pornography). Copyright cases were limited to violations of rights in images or literary works.[345] Issues with massive illegal downloading of music and videos through peer-to-peer file sharing or the sharing of such material through platforms did not arise before the start of the new millennium.

Nevertheless, the characteristics of the internet and digital technology already posed an entirely new regulatory challenge. Matters of jurisdiction, detection and enforcement became more complex. Originators of information could easily remain anonymous. Perpetrators could avoid law enforcement authorities through removal or relocation of content into other jurisdictions. Prosecuting consumers for accessing or downloading infringing

343 For a comprehensive overview by different EU jurisdictions and in the US regarding the liability of ISPs for third party content prior to the ECD, see: Gerald Spindler and Fritjof Börner (eds), *E-Commerce Law in Europe and the USA* (Springer 2002); Leistner (n 336) 89. and Verbiest and others (n 315) 22, 57.

344 Waisman and Hevia (n 313) 785.

345 Davies (n 27). Mayer-Schönberger and Foster (n 96).

material or products was likewise inefficient. Digitisation, in connection with the new nature of the internet, meant that copyrighted material could be multiplied, accessed and distributed widely, instantaneously and without loss in quality.[346]

When faced with these new legal challenges, courts responded in different ways. Many of these early cases dealt with IAPs which acted either as conduits or hosts for unlawful content, or both. They mostly ran newsgroups or bulletin boards through which their users shared information in texts and images. An illustration of cases prior to the creation of dedicated intermediary liability provisions gives a useful insight into the underlying diversity of legal approaches and interpretations of the roles and responsibilities of these new actors. Some basic controversies, such as whether intermediaries can be considered editors, what responsibilities they have in preventing unlawful activity, or the effect of their intermediation on substantive aspect of law governing the material in question, remain or have re-emerged as central liability issues.[347] This poses the question of whether the legal regimes that developed out of the cases discussed below have been fully effective and future proof. The following review shall also serve as an outline of key trends and the variety of possible ways of assessing and allocating liabilities and responsibilities for the new practices of information intermediation that emerged on the internet.

I. Case law in the EU

In Europe, many of these cases reflected a general perception that intermediaries should be made directly liable for unlawful content posted on their networks, in particular where they undertook efforts to monitor for infringing material or where they were notified of the potentially unlawful nature of content.

a. United Kingdom

In one of the first cases brought against an internet intermediary in Europe, an UK court found that the IAP *Demon Internet* was liable as a publish-

346 Hector L MacQueen and others, *Contemporary Intellectual Property: Law and Policy* (2nd ed, Oxford University Press 2011) 240–242.

347 Lipton (n 287) 1350.

er for defamatory content posted on one of its newsgroups.[348] The judge rejected the defendant's claim that they were *"merely owners of an electronic device through which postings were transmitted."* Instead, the defendant "*chose to store…postings within their computers."*[349] Having been found a publisher, the defendant had to pass the liability test of the 1996 UK Defamation Act,[350] which it failed because it did not react to notices received by the plaintiff concerning the defamatory nature of the content. It therefore did not take reasonable care and failed the knowledge test after receiving the notice. Regarding the knowledge test, the court called on a 1937 judgement[351] in which a golf club operator failed to remove defamatory content from one of its noticeboards. The case appears to construct a combination of vicarious and contributory liability, by combining elements of control and actual knowledge. The actual knowledge test was only applied once the defendant was found to be a publisher. The outcome of this case has been interpreted as obliging an IAP to monitor proactively for potentially unlawful information that passes through its system.[352]

The tendency of holding internet hosts liable for information posted on their sites was continued in the rulings of *Sir Elton John v Countess Joulebine*[353] and *Totalise v Motley Fool.*[354] In the former case the website provider was liable because they ought to have known that the information posted was privileged, and consequently released onto an online newsgroup under a breach of confidence. Meanwhile in *Totalise*, an IAP was ordered to disclose the identity of an anonymous user who had posted defamatory material.

348 *Godfrey v Demon Internet Limited* [1999] High Court Of Justice Queen's Bench Division 998-G-No 30, EWHC QB 244.
349 ibid 35.
350 Defamation Act 1996 c.31 1996 s 1.
351 *Byrne v Deane (1937)* 1 KB 818.
352 Charlie Wood and others, 'Great Britain' in Gerald Spindler and Fritjof Börner (eds), *E-commerce law in Europe and the USA* (Springer 2002) 291.
353 *Sir Elton John and others v Countess Joulebine and others [2001] MCLR 91* (Unreported).
354 *Totalise Plc v The Motley Fool Ltd & Anor [2001] EWHC 706 (QB) (19 February 2001)* (Unreported).

b. Germany

In Germany, the ISP *CompuServe* was initially successfully prosecuted for facilitating access to child pornographic material through its newsgroups.[355] In 1998, its managing director, *Felix Somm*, incurred criminal charges for facilitating the distribution of illegal materials and for failing to block access to them despite being notified of illegal content by German authorities. The decision was reversed one year later, noting that *CompuServe GmbH*, the German subsidiary of the US based group, did not have control over the information posted. Once it had gained knowledge, it was not in a position to physically remove the materials from the US-based servers. Meanwhile, existing German law at the time would have also protected *Somm* and the German subsidiary of *CompuServe Inc.* It was noted that the German laws were in compliance with the ECD, which was to become EU law one year later.[356]

In *CD Bench*, the Munich Upper Regional Court had to decide whether the operator of a File Transfer Protocol (FTP) server was liable for and had to stop and prevent the allegedly illicit download of software hosted on its system.[357] The FTP operator, a university, mirrored the content of seven software archives, containing around 40,000 pieces of software on its servers and offered unrestricted access to it. The Munich court first ruled that the University was not responsible for content hosted on its FTP server if it did not have any influence over that content. Secondly, it would only be liable if it had "positive knowledge", therefore presuming at least partial intent of the fact that it hosted illicit content. Thirdly, liability would then only arise if it was technically reasonable to prevent these downloads. The Munich Court saw control (influence) and knowledge as preconditions for liability. The most controversial issue was, however, whether it was reasonable to expect that the operator prevent downloads of illicit content. The Court answered in the negative. It found that in the absence of a technical solution a manual review of 40,000 software packets for infringing software was unreasonable. The technical and economic effort did not justify the limited effectiveness of the measures.[358] The assessment of the

355 *CompuServe* [1998] AG München 8340 Ds 465 Js 173158/95, MMR 1998, 429.

356 Lothar Determann, 'Case Update: German CompuServe Director Acquitted on Appeal' (1999) 23 Hastings International and Comparative Law Review 17, 123.

357 *CDBench, 6 U 5475/99* [2000] MMR 2000 617 (OLG München).

358 *CDBench, 6 U 5475/99* [2000] MMR 2000 617 (OLG München) [619]; Wulff-Axel Schmidt and Monika Prieß, 'Germany' in Gerald Spindler and Fritjof Börner (eds), *E-commerce law in Europe and the USA* (Springer 2002) 216.

proportionality of preventive measures was to be developed further by German courts in the years to come.

c. France

Union des étudiants juifs de France (UEJF) et La Ligue contre le racisme et l'antisémitisme (LICRA) v Yahoo Inc et Yahoo France[359] was one of the more high-profile early cases on the liability of internet intermediaries in the EU that took place prior to the enactment of the ECD. Decided in 2000, US ISP *Yahoo* was successfully prosecuted for making Nazi memorabilia, hosted on an auction site on its US servers, available for purchase to residents in France. The sale and possession of these materials is prohibited under the French penal code. The Paris court did not call into question *Yahoo.fr's* involvement in enabling the marketing of these goods by providing a link to the US site on *Yahoo.com* from its search engine. The judges ordered *Yahoo.com* in the US to disable access to the illegal memorabilia in question for users accessing the site from France. The judges found that it was possible to identify the country-of-origin of 70% of users from the IP address. An IP based block (geo-blocking) of France-based users would be technically possible and effective.

Meanwhile *Yahoo.fr* was ordered to warn all users of the illegality of these acts who, based on use of its search engine or other activity, were provided with a link to infringing material on *Yahoo.com*.[360] The decision concerning *Yahooo.com* was overturned by a US court five years later. The court rejected the notion that a French court should have a say over the regulation of speech in the US.[361]

The French law on liability for third party content received several iterations prior to the ECD. The above judgement reflects a situation of legal uncertainty at the time over the liability of IAPs and hosts for the material

359 *UEJF and Licra v Yahoo! Inc and Yahoo France* (2000) (Unreported) (Tribunal de Grande Instance de Paris).

360 For a detailed analysis see: Carolyn Penfold, 'Nazis, Porn and Politics: Asserting Control Over Internet Content' (2001) 2 The Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-2/penfold.html> accessed 2 October 2019.

361 *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme* [2006] 9th Cir 2006 01-17424, 433 F.3d 1199.

hosted or referenced through their services.[362] While *Yahoo.com* was not incriminated for intentionally infringing acts, there was little question over it being liable for the sale of products offered by third parties in France. Likewise, *Yahoo.fr's* search engine and hosting services were ordered to warn users without any debate having taken place over the liability for the actions of third parties.

These uncertainties are also displayed in a 1999 case involving privacy and image rights of a fashion model, who had nude pictures of her posted on several websites.[363] Stocking images and making them accessible to others conferred on the four hosting providers in question professional diligence and duty of care obligations, which they had breached. Apart from clear terms and conditions that indicated the prohibition of illicit acts, the hosts would have had to prevent the availability of manifestly unlawful material on their sites. Putting in place an internal word search that was able to detect manifestly unlawful content was deemed as technically feasible and in line with principles of freedom of expression. Likewise, failure to notify and warn the editors of the existence of illicit material was a breach of professional duties. The court lamented on the lack of state regulation and nascent self-regulation in this area, which necessitated reference to the standards laid down in the Code Civil (the then Article 1382).

d. Italy

Italian judgements provide two conflicting interpretations on the liabilities of internet intermediaries for third party content.[364] This is certainly due to the less clearly expressed concept of contributory liability mentioned above,[365] combined with the new challenges posed by the internet. In a number of cases in the late 1990s Italian judges have, on the one hand, found that an IAP acted as an editor. It had therefore a duty to verify the

362 Isabelle Renard and Marie Amélie Barberis, 'France' in Gerald Spindler and Fritjof Börner (eds), *E-commerce law in Europe and the USA* (Springer 2002) 133.

363 *Madame L v les sociétés Multimania Production, France Cybermedia, SPPI, Esterel* (1999) (Unreported) (Tribunal de Grande Instance de Nanterre).

364 Massimiliano Mostardini, Luigi Neirotti and Massimo Travostino, 'Italy' in Gerald Spindler and Fritjof Börner (eds), *E-commerce law in Europe and the USA* (Springer 2002) 368–371.

365 Bertolini, Franceschelli and Pollicino (n 339) 141–145.

lawfulness of the content lest it be found guilty of negligent behaviour, thus causing contributory liability for facilitating illegal acts.[366]

By contrast, other decisions rejected the editor-analogy and added that it would be technically impossible for an IAP to check all the content it transmitted or hosted.[367] Commentators at the time also criticised the jurisprudence for not distinguishing between IAPs and hosting providers. Each business model results in different levels of control over content, which could be decisive for whether civil liability existed or not.[368]

e. Belgium

Belgium Courts have tended to find IAPs and internet hosts liable for third party content prior to the ECD. For example, a bulletin board was found responsible for copyright infringing material on its site and charged with monitoring the postings of its users' activities for further infringing material.[369] Likewise, an IAP was found responsible for providing access to illegal content on third party websites.[370] Courts found IAPs and hosting providers liable as contributors under tort, unfair competition, copyright and trademark law.[371]

The outcomes of the cases above offer an interesting diversity of approaches towards the liability of intermediaries. Intermediaries were occasionally charged with primary or strict liability for the acts performed by third parties. Where they were not found to be editors there does not seem to be a coherent line of argument over when vicarious or contributory liability would be attributed. This may have to do with the fact that secondary liability is differently construed in the different Member States. Secondly, it appears that there is a high degree of uncertainty over the level

366 see *Order of the Tribunal of Napoli on 8 August 1997*; *Order of the Tribunal of Roma on 22 March1999*; in: Mostardini, Neirotti and Travostino (n 339).

367 *Order of the Tribunal of Cuneo on 23 June 1997*; *Order of the Tribunal of Roma on 4 July 1998*; in: Bertolini, Franceschelli and Pollicino (n 317) 144; and in: Mostardini, Neirotti and Travostino (n 339) 369.

368 Mostardini, Neirotti and Travostino (n 363) 369.

369 *Cour d'Appel d'Anvers, 28 février 2002* (2002) (Unreported). in: Verbiest and others (n 315) 50.

370 *Cour d'Appel de Bruxelles, 13 février 2001* (2001) (Unreported); Benoit Michaux and Stefan Van Camp, 'Belgium' in Gerald Spindler and Fritjof Börner (eds), *E-commerce law in Europe and the USA* (Springer 2002) 56.

371 Michaux and Van Camp (n 369) 56.

of control and knowledge intermediaries have over the information on their systems. Thirdly, uncertainty exists over what standard of control and knowledge intermediaries should be expected to have from a moral, technical and legal standpoint.

These cases also reflect the relatively one-dimensional scope of the intermediary landscape at the turn of the millennium. The vast majority of legal challenges is directed at ISPs, which mainly act as infrastructure and communication network providers, and, in some, instances as hosting platforms for content and information.

II. Case in law in the US

A short overview of US case law provides a useful illustration of the commonalities and differences to the developments in the EU. In the US, the first cases on intermediary liability had emerged by the middle of the 1990s. This does not come as a surprise considering that the country was the pioneer in user adoption and commercialisation of the internet. Arguably, this precedence helped inform the legislator in its design of a regulatory framework for intermediary liability.

a. Cubby, Inc v CompuServe, Inc.

The earliest case involving the liability of an intermediary was *Cubby, Inc v CompuServe, Inc (Cubby)*,[372] which dealt with defamatory content and was decided in 1991. *CompuServe* was an early IAP that also ran an online information service in the form of an electronic library which contained over 150 special interest fora. One of these fora was dedicated to journalistic content and run and managed by a media company subcontracted by *CompuServe*. Defamatory content appeared on the forum in question, posted by a content provider working for the forum operator. The plaintiffs argued that *CompuServe* carried the defaming statements and was a publisher thus incurring a higher standard of liability than a distributor. *CompuServe* rejected the charges claiming it had no control over the entities responsible for the forum's content nor had it been notified of any defamatory statements.

372 *Cubby, Inc v CompuServe Inc*, (1991) 776 F. Supp. 135 (SDNY).

The New York judges reviewed *CompuServe's* business model and agreed, finding that it could only be judged by standards that apply to distributors of publications, but not editors. They likened *CompuServe* to a library or bookstore. Consequently, *CompuServe* was protected under the US Constitution's First Amendment which guarantees freedom of speech and freedom of press. The adequate liability standard applying to CompuServe was "whether it knew or had reason to know of the allegedly defamatory […] statement."[373] However, no evidence was provided that substantiated that *CompuServe* was in a position to have this knowledge. The judges also rejected claims of vicarious liability. The media company running the news forum acted merely as an independent contractor of *CompuServe*, with all editorial control being delegated to the former. Likewise, the entity posting the comments had no contractual relationship whatsoever with *CompuServe*.

b. Stratton Oakmont v Prodigy Services Co.

Stratton Oakmont,[374] the plaintiff, was an investment firm that filed a libel claim for defamation against *Prodigy Services*, a computer network which hosted bulletin boards and had a subscriber base of 2 million users at the time. One of these boards carried defamatory statements against *Stratton*. The latter alleged that *Prodigy* acted as an editor of information and was therefore responsible for the defamatory comments made. *Stratton* rested its claim on the fact that *Prodigy* actively promulgated and enforced its content policies and used software to pre-screen publications for offensive content.

The judges agreed with the plaintiff. *Prodigy's* conscious choice to monitor and censor communication and invest in technology and staff to enable these activities made it an editor. The court also tried to disperse fears that this could motivate bulletin board hosts to abandon any control over communications lest they would incur full liability. Market demand, they presumed, would reward those providers that choose to police content and therefore risk higher exposure in order to offer value added services, such as a family-friendly communication environment, like *Prodigy's*.

373 ibid 141.
374 *Stratton Oakmont, Inc v Prodigy Services Co* (1995) 1995 WL 323710 (NY Sup Ct).

While described as irreconcilable with the *Cubby* ruling,[375] the judges in *Stratton* explicitly stated that they fully agreed with the principles in *Cubby*. However, while both *CompuServe* and *Prodigy* were seen as computer bulletin boards, it was the latter's conscious choice to "regulate" the content on its boards that exposed it to a higher standard of liability, which in this case was equal to editorial control. The judges may, however, have underestimated that the combined business risk of investing into content management and incurring higher liabilities could act as a serious deterrence for internet businesses at the time. Another way of reading it is, that a provider that engaged in good faith efforts to prevent illegal acts would incur higher liability than one that allowed all and every content to circulate unchecked on its systems. The decision was criticised on these grounds and had an important influence on the Communications Decency Act, which was to be passed one year later.[376]

c. Playboy Enterprises, Inc. v Frena

Copyright was another area that eventually moved into the limelight of courts due to the emergence of the internet and its intermediaries. The internet posed an existential challenge to copyright, since at its core it relies on the act of copying and sharing of information. As such, digitisation and the internet affect the substance of copyright law.

In *Playboy Enterprises, Inc. v. Frena*, the eponymous magazine charged the operator of a bulletin board, Mr. Frena, with copyright violation. Users of *Frena's* service could, for a fee, view, and up- and download photos to and from various directories stored on the bulletin board. *Playboy* held the copyright in some of these images and claimed that its rights were violated by the unauthorised sharing of these images. *Frena* contradicted this by stating that he was not aware of the images having been uploaded by its users and that he removed them once notified of their existence. The court found *Frena* directly liable for copyright infringement. It held that "intent

375 Bryan J Davis, 'Comment: Untangling the "Publisher" versus "Information Content Provider" Paradox of 47 u.s.c. § 230: Toward a Rational Application of the Communications Decency Act in Defamation Suits against Internet Service Providers' (2002) 32 New Mexico Law Review 75.

376 Citron and Wittes (n 197) 456–458; Felix T Wu, 'Collateral Censorship and the Limits of Intermediary Immunity' (2011) 87 Notre Dame Law Review 293, 313–317.

or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement."[377]

d. Sega Enterprises, Ltd. v MAPHIA & Religious Technology Center v Netcom

This somewhat harsh judgement was toned down in *Sega Enters., Ltd. v. MAPHIA*[378] which concerned the distribution of copyright protected video games through a bulletin board operated by *Maphia*. In contrast to *Frena*, the courts found in *Sega* that the bulletin board operator was only liable for contributory infringement. *Maphia's* system was merely used by another party to commit the copyright breaches. The acts lacked therefore volition or causation, which would be necessary elements for a direct infringement claim to be successful.[379] In *Maphia*, the court applied reasoning from a previous ruling, *Religious Technology Center (RTC) v Netcom.*[380]

Netcom has been seen as establishing a line of argument that holds IAPs liable for contributory infringement in copyright disputes involving internet intermediaries.[381] The plaintiff *RTC* had asked IAP *Netcom* to stop a user on a bulletin board operated by another party on *Netcom's* system. The user had posted allegedly copyright infringing materials. However, *Netcom* refused to block access of the user, claiming this would unduly restrict other users on the Bulletin Board in question. It also claimed that it was impossible to pre-screen the postings of the user. Although technically possible, *Netcom* chose not to bring in filtering systems nor did it chose to archive or control traffic or content on its systems. The judges found that in the absence of control over the information passing through Netcom's system it would be an unduly broad construction of copyright to hold the company directly liable.[382] Therefore the important precedence this case established was that, no matter whether an intermediary proactively

377 *Playboy Enterprises, Inc v Frena* (1993) 839 F. Supp. 1552 (MD Fla) [1559].
378 *Sega Enterprises Ltd v MAPHIA* (1994) 857 F. Supp. 679 (Dist Court, ND Cal). & *Sega Enterprises Ltd v MAPHIA* (1996) 948 F. Supp. 923 (Dist Court, ND Cal).
379 *Sega Enterprises Ltd v. MAPHIA* (n 377) para 932.
380 *Religious Technology Center v Netcom On-Line Com* (1995) 907 F. Supp. 1361 (Dist Court, ND Cal).
381 Schruers (n 330) 110–112.
382 *Religious Technology Center v. Netcom On-Line Com.* (n 379) s 1372.

worked to prevent or investigate infringement claims, it would be subject to contributory infringement.[383]

The rulings of these early cases already demonstrate the diverse and fluid nature of facts and arguments involved when trying to pin down the obligations of intermediaries on the (new) internet. In the EU, distinct national traditions of secondary liability and varying interpretations of the role of the different internet intermediaries in hosting different kinds of unlawful content led to diverging rulings and calls for regulatory clarification.[384] In the US, a tendency of allocating certain protections against primary liability to these new intermediaries appeared to crystallise. However, the legal conditions for such outcomes were far from established.[385] Given the rising importance of the internet as a means for expression and as a commercial and economic factor, many countries in the world undertook to establish statutory rules for the obligations of online intermediaries. This will be discussed in the following section.

C. *Regulatory Frameworks of internet intermediary liability*

1. US

A discussion of intermediary liability law anywhere in the world would be incomplete without at least a short account of the US regulatory framework. Apart from its technical origins, the internet as a commercial endeavour also broke ground in the US. As shown above, this gave rise to the earliest legal disputes between new internet actors, users and rightsowners.

The need to codify the conditions under which internet intermediaries would be held liable arose out of several considerations. First, the US common law system of secondary liability, which would be applicable to the activities of internet intermediaries by default, is very complex. The different liability standards (e.g. contributory and vicarious liability) are applied in nuanced ways depending on the type of offense and legal area, varying between copyright, trademark or defamation law.[386] Given the rapidly de-

383 Schruers (n 330) 111.

384 As shown above in the case of: *Madame L. v. les sociétés Multimania Production, France Cybermedia, SPPI, Esterel* (n 362).

385 Andrej Savin, *EU Internet Law* (Second edition, Edward Elgar Publishing 2017) 152.

386 Salil K Mehra and Marketa Trimble, 'Secondary Liability of Intermediary Service Providers in the United States: General Principles and Fragmentation' in

veloping internet sector, this did not bode well for consistency of court rulings and predictability for this still volatile sector. Secondly, and partly as a result, the emerging internet intermediary industry had started to convince the legislator successfully that legally mandated limitations for content liability were necessary in order to safeguard the future of the internet.

Both in the US and the EU, intermediaries portrayed themselves as mere conduits and access providers. They stored files, web pages or email accounts for users and businesses on their servers. But they did not hold themselves to be content providers.[387] Indeed the early case law seemed to support this. Most early legal disputes concerned the likes of *CompuServe*, *Demon Internet*, *Yahoo* or *Netcom*. The emerging liability rules were influenced by these perceptions of online intermediaries.

I. Communications Decency Act 1996

The US decided for sectoral regulation of intermediary liability. The Communications Decency Act's Section,[388] which was put in place as section 230 of the Telecommunications Code in 1996, regulates the liabilities of "interactive computer services" for any offensive material.[389] This covers a broad array of claims, from defamation and discrimination to unfair competition.[390] The definition of an interactive computer service provider is sufficiently large to include any internet intermediary service that provides internet access and content storage and does not, at the same time, act as an information content provider. The CDA provides pure intermediaries with a blanket exemption from any liability over content provided by third parties. The famous "Good Samaritan" provision[391] exonerates internet intermediaries from being treated as a speaker or publisher, thus excluding primary liability for any information provided by another content provider. At the same time, it protects intermediaries from any secondary liability where these undertake voluntary measures in good faith, that aim to restrict the availability of offensive material and assist content providers

---

Graeme B. Dinwoodie (ed), *Secondary liability of internet service providers* (Springer Berlin Heidelberg 2017) 94–99.

387 Edwards, 'The Fall and Rise Of Intermediary Liability Online' (n 119) 60–61.

388 47 USC § 230. The detailed name 47 USC 230: "Protection for private blocking and screening of offensive material".

389 ibid 230 (c).

390 Ardia (n 129) 379.

391 47 USC § 230 s 230 (c).

in these efforts. This resulted in a broad safe harbour for the activities of internet intermediaries in the US. The protection does not, however, extend to any violation of US federal criminal statutes, such as for example material harmful to minors or content and communications relating to the sexual exploitation of children.[392]

The policy objectives of the CDA were clear: promote and protect a nascent and vibrant internet industry against liability risks during an essential phase of business expansion. The 2000 dot.com crash four years later was to serve as a reminder of the precariousness of many early internet business models. Still, policy makers wanted to encourage the industry to protect users, and especially children, against the worst excesses of unlawful, objectionable and offensive content on the internet. Conscious of the ambiguity of making decisions on speech and the broad protections afforded by the US Constitution in that respect, they therefore protected intermediaries against any mistakes when removing content as part of their good faith efforts. In addition, they wanted to assure that the knowledge accrued through voluntary content policing could not be turned against these intermediaries, as happened in the *Prodigy* case. The CDA was in line with the US Government's philosophy that regulation should be light touch and based on voluntary industry commitments.

No further analysis shall be given here of the effectiveness and consequences of this crucial piece of law on intermediary liability. Suffice it to state that it engendered a significant body of case law.[393] The majority of cases grapple with the rather blunt distinction between interactive computer services and content providers. Courts also felt compelled to investigate in more detail the degree of control and influence intermediaries had on content. The outcome of these inquiries would, of course, have an effect on the availability of the safe harbour defence. Case law appeared to become more frequent after 2003. This coincides with the emergence of Web 2.0 and the increasingly interactive and intrusive role of new types of intermediaries in the intermediation of content.

The debate over the CDA has become fiercer ever since. On one side of the spectrum it has been criticised as overshooting its target and intrusively regulating speech.[394] On the other side, the US Government's traditional

392 'Section 230 of the Communications Decency Act' <https://www.eff.org/issues/cda230> accessed 8 October 2019 (e) (1).

393 Ardia (n 129).

394 Raymond SR Ku and Jacqueline D Lipton, *Cyberspace Law: Cases and Materials* (2nd ed, Aspen Publishers, Inc 2006) 112–115.

hands off approach towards intermediaries is blamed for unduly protecting the practices of internet giants which have long ceased to be neutral intermediaries.[395] Yet others see the CDA as a guarantor of free expression on the internet.[396] However, while the broad anti-indecency provisions of the CDA had been successfully challenged by several court rulings,[397] the safe harbour passage of section 230 has remained largely intact. The only major change to this statute was made in 2018, when acts that facilitate sex trafficking were exempted from the protections offered by the CDA.[398] The US Government under President Trump moved to break, however, with this traditional light touch approach towards intermediary regulation. A review of the CDA by the US Congress, published in 2020, resulted in proposals that would see the current liability immunities being reduced significantly where it concerns content that relates to illegal drugs, child abuse, cyberstalking or terrorism.[399]

II. The Digital Millennium Copyright Act 1998

The DMCA[400] introduced a separate liability regime to the existing US Copyright code, targeting breaches of copyright committed via the internet. Section 512 DMCA, also called the safe harbour provisions, creates a somewhat higher standard of intermediary liability exemptions than compared to the CDA for speech violations. Section 512 creates four categories of intermediaries: a) service providers that merely transmit, route or transmit information – this would be IAPs under the typology offered in the previous chapter; b) services that cache information;[401] c) services that

395 Zuboff (n 5) ss 2015–2058.
396 'Section 230 of the Communications Decency Act' (n 391).
397 Amongst others by *Reno v American Civil Liberties Union* [1997] US Supreme Court 96-511, 521 US 844.
398 The Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) amend the CDA 47 USC § 230 (e) (5).
399 US Department of Justice's, 'Department of Justice's Review of Section 230 of the Communications Decency Act Of 1996' (2020) <https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996> accessed 7 October 2020.
400 17 U.S.C. § 512.
401 Caching is an intermediary storage of information in hardware during the data transmission process on the internet, which happens for the sole purpose of retrieving future; similar information requests faster. It is a form of buffering.

store information at the request of a third party – these services are referred to as hosting services, and d) information location tools that link or refer users to another online location, i.e. search engines.[402]

All of these service providers need to act at the direction of third parties as a precondition in order to afford the safe harbours.[403] Information hosts and search engines have to meet a knowledge standard in order to avail themselves of (secondary) liabilities for copyright infringement. They must not have actual knowledge of infringing activity or must not be aware of any circumstances from which infringing activity is apparent. Once aware or in possession of such knowledge they need to remove infringing information or access to it expeditiously.[404] This "red flag" knowledge, which the company acquires in the course of its business, would need to stand a subjective and an objective test. The former would try to establish whether the intermediary had actual knowledge under the concrete circumstances. The objective test would then verify whether the knowledge was indeed "red flag" knowledge, i.e. whether to a reasonable person acting under the same circumstances the infringing nature of the activity would have been (blatantly) obvious.[405]

This test has become one of the more contentious issues. The exact circumstances of when the more complex and interactive intermediaries of today have actual, i.e. specific, knowledge of an infringing activity are notoriously difficult to establish by courts across the globe.

Knowledge can also be attained through notifications of a claim of infringement. The format, content and procedure for such notifications are laid down in detail under a notice-and-take-down process, which includes provisions for counter-claims.[406] The latter tries to limit the potential chilling effect from indiscriminate removal of content by intermediaries anxious to avoid liability. At the same time, intermediaries are freed from any liability against properly administered, but erroneous takedowns,[407] which

---

James Bottomley, 'Understanding Caching' [2004] Linux Journal <https://www.linuxjournal.com/article/7105> accessed 8 October 2019.

402 17 U.S.C. § 512 (a) - (c).

403 System caching services shall not be treated here in detail as there has been little controversy over their intermediary status and liabilities.

404 17 U.S.C. § 512 (c)(1) (A) - (C), (d) (1) (A) - (C).

405 'House of Representatives - Digital Millennium Copyright Act of 1998' (1998) Rept. 105–551 53.

406 17 U.S.C. § 512 c (3).

407 ibid (g)(1).

can be seen as an equivalent to the "Good Samaritan" protection afforded under the CDA.

Hosts can not avail themselves of these liability protections if they derive a direct financial benefit from infringing activities. The definition of direct financial benefit has become more difficult in the wake of Web 2.0 business models,[408] such as *YouTube*, which would "only" generate ad revenue from the display of copyright infringing content on its site.

Finally, the DMCA affords a limited array of injunctive relieves against intermediaries and does not allow for any monetary relief.[409]

Similar to recent initiatives to weaken the safe harbour protections of the CDA, the current US Government has also voiced its intention to roll back key protections afforded to internet intermediaries against copyright infringements conducted via their systems.[410] This will be mentioned in more detail in the section on copyright in Chapter 4.

III. Trademarks – The Lanham Act

Internet intermediaries have affected trademark law in several ways. First, cybersquatting concerns the registration and use of domain names that are confusingly similar to trademarks for abusive purposes. Secondly, since the rise of the commercial search engine, advertisers have used keywords of brands to display products of competitors to consumers. Thirdly, online marketplaces have been utilised by sellers offering imitations or counterfeits of successful, often prestigious, brands.

US trademark law (the Lanham Act)[411] had traditionally not dealt with secondary or indirect infringement. These kinds of conflicts are resolved by the owner of the mark, who directly pursues the infringer. Contributory liability in trademark infringement was only confirmed by the US Supreme Court in 1982.[412]

---

408 Rowland, Kohl and Charlesworth (n 128) 96.

409 17 U.S.C. § 512 (j).

410 'Section 512 of Title 17 - A Report of the Register of Copyrights' (United States Copyright Office 2020) <https://www.copyright.gov/policy/section512/> accessed 29 June 2020.

411 The Lanham (Trademark) Act 1946 (15 USC § 1051 et seq).

412 *Inwood Laboratories Inc v Ives Laboratories, Inc*, (1982) 456 U.S. 844 (United States Supreme Court). In: Jasmine Abdel-Khalik, 'Is EBay Counterfeiting?' in Hannibal Travis (ed), *Cyberspace law: censorship and regulation of the Internet* (Routledge 2013) 144;

As cybersquatting became more of a problem, the US passed the Anticybersquatting Consumer Protection Act (APCA)[413] in 1999 as an amendment of the Lanham Act. This statute charges domain name registrars and registries with liability for injunctive or monetary relief only where they fail to expeditiously comply with a court order concerning a fraudulent domain registration.

Apart from this, no specific statutory provision protects online intermediaries in trademark infringement cases. US courts have instead sought to apply direct infringement tests as well as the knowledge standard tests for contributory infringement in cases against search engines[414] or online marketplaces.[415] Both types of liability claims have generally been unsuccessful. Regarding contributory infringements, it is worth noting that, where online intermediaries acted on specific infringements notified by rightsowners, they were generally vindicated. US courts have applied a high bar to the standard of general knowledge over infringing activity.[416] It appears that for trademarks courts have arrived at similarly broad intermediary protections as in those guaranteed through the safe harbour provisions in the DMCA.

2. EU

I. Setting the scene for an intermediary liability framework

From 1996 the EU started to formulate a strategy aimed at capturing the opportunities of the internet and e-commerce for Europe. The 1996 Rolling Action Plan[417] and the 1997 Communication on "A European Initiative in Electronic Commerce"[418] brought together a number of separate

413 Anticybersquatting Consumer Protection Act (ACPA) (15 USC § 1125(d)).
414 *Rosetta Stone Ltd v Google, Inc* (2012) 676 F 3d 144 (4th Cir).
415 *Tiffany (NJ) Inc v eBay Inc* (2010) 600 F. 3d 93 (2nd Cir).
416 *Rosetta Stone Ltd. v. Google, Inc.* (n 413) para 163. *Tiffany (NJ) Inc. v. eBay Inc.* (n 414) para 107. And the detailed discussion of *Tiffany* in: Abdel-Khalik (n 411) 47–57.
417 European Commission, 'Communication from the Commission on" Europe at the Forefront of the Global Information Society: Rolling Action Plan", COM(96) 607 Final' (1996).
418 European Commission, 'Communication from the Commission: A European Initiative in Electronic Commerce, COM(97) 157 Final' (1997)

policy initiatives into a broad strategy.[419] It was aimed at promoting investments in technology and infrastructure, a favourable business environment, making a proactive impact on global cooperation and creating a coherent regulatory framework for e-commerce in the single market[420] as the EU entered the new millennium.

The EU had addressed the problem of illegal and harmful content on the internet in a separate Communication in 1996,[421] which recognised the variety of illegal and harmful content online and the need for innovative and differentiated legal and technological responses. This Communication acknowledges Member States' responsibility for applying their national laws to the new online environment but warned against diverging legal responses by national legislators. There was a risk that national solutions distorted competition, hampered the free movement of services and fragmented the internal market.[422]

The Commission did not appear to actively plan for an EU liability framework at that stage. It did, however, explore EU wide action as one policy option in conjunction with more industry self-regulation. It also encouraged Member States to come together and lay down minimum standards on criminal content.[423] However, it threatened with direct regulatory intervention should national legal solutions start to generate market fragmentation.

II. The E-Commerce Directive

a. General principles and scope

Two years after its Communication on illegal and harmful content on the internet, in December 1998, the Commission submitted a proposal for the

419 There were, for example, Information Society Initiatives on standardisation, education, illegal and harmful content, social and regional policy, infrastructure, market liberalisation, research and investment, and more.

420 European Commission, 'Communication from the Commission: A European Initiative in Electronic Commerce, COM(97) 157 Final' (n 417) 1–2.

421 European Commission, 'Communication from the Commission: Illegal and Harmful Content on the Internet, COM(96) 487 Final' (1996) <https://core.ac.uk/reader/5078710> accessed 9 October 2019.

422 ibid 4–5.

423 ibid 24–25.

ECD.[424] The ECD finally became EU law on 8 June 2000 as *Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*. Based on the objectives in the European Initiative on Electronic Commerce, it approximates EU Member States' laws in several areas, one of which being the liability exemptions accorded to internet intermediaries. The additional areas include national provisions of information society service providers, the establishment of service providers, commercial communications, electronic contracts, code of conducts and the cooperation between Member States.[425]

The preoccupation to remove cross-border obstacles within the single market could serve as one explanation for the broad horizontal regime the ECD sought to establish. The shared legislative competence of the Directive is derived from Articles 47(2), 55 and 95 of the EC Treaty, now corresponding to Articles 53 (1), 62 and 114 of the Treaty of the Functioning of the European Union (TFEU).[426] Article 53 concerns provisions aimed at persons that want to take up and pursue activities as self-employed persons. It allows the EU to issue directives aimed at stipulating conditions for the mutual recognition of professional qualifications under the freedom of establishment. Article 62 provides shared competences in the area of the provision of services. Finally, Article 114 confirms the remit of the ECD as a legal instrument adopted as part of the shared, and therefore limited, competence of the EU as detailed in Article 4 (2) TFEU.

Accordingly, the Directive rests on the principle of proportionality and therefore pursues a minimum harmonisation approach. This means it lays down only measures that are strictly needed for the operation of the internal market and the safeguard of general interest principles, particularly the protection of minors, human dignity, consumers and public health.[427] The Commission tried to avoid overregulation.[428] This is underlined by commitments in the ECD to light touch regulatory intervention, specifically the use of self-regulatory measures. Article 16 and 17 of the ECD emphasise the promotion and creation of voluntary codes of conduct by industry,

424 European Commission, Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market 1999 [1999/C 30/04].

425 Directive 2000/31 (ECD) Article 1 2.

426 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) 2016 (OJ C 202).

427 Directive 2000/31 (ECD) Recital 10.

428 Büllesbach (n 51) 295.

professional and consumer associations, as well as the use of out-of-court settlement procedures.[429]

The ECD seeks to create a harmonised regulatory environment for information society service providers (ISSPS). ISSPs had been defined under the Technical Standards and Regulations Directive in 1998 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[430]

ISSPs' activities are regulated by the country-of-origin principle. The country-of origin-principle in Article 3 (1) obliges Member States to ensure that ISSPs comply with the laws of the Member State in which they are established throughout the territory of the EU. The non-discrimination principle in Article 3(2) precludes Member States from restricting the freedom to provide information society services from any other Member State.[431] This means that services covered by the ECD will only need to follow the rules of the Member State in which they are established. This straightforward use of the country-of-origin principle can be attributed to the EU's desire to establish a regulatory framework for electronic commerce that is harmonised.[432]

On the other hand, the impracticalities of the strict country-of-origin rule come to the fore when courts need to enforce certain decisions, such as for example information requests against ISSPs, including online intermediaries. National or local authorities are, strictly speaking, required to approach the EU jurisdiction where the entities are established, even where subsidiaries may exist in their own country.[433] This may cause additional administrative burdens. The country-of-origin principle in the ECD

429 Directive 2000/31 (ECD) Articles 16 and 17.

430 Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations 1998 (OJ L 217) Article 1 2. (a). This was later amended by Directive 2015/1535/EU of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

431 Directive 2000/31 (ECD) Article 3 1. & 2.

432 Rowland, Kohl and Charlesworth (n 128) 268–269.

433 *Auskunftsanspruch über persönliche Daten von Nutzern einer Onlineplattform wegen des Verdachts der Zweckentfremdung von Wohnraum* [2017] VG Berlin 6 Kammer 6 L 162.17, DE:VGBE:2017:07206L162170A at 33 - 39. In this case, brought against a local branch of *AirBnB,* Berlin authorities were denied an information disclosure order. The administrative court of Berlin applied the ECD's country-of-origin principle by ruling that the order would need to be filed against *AirBnB's* EU seat of establishment in Ireland.

has therefore been seen as encompassing a conflict of law rule because it directs towards the law of the seat of establishment of the ISSP.[434]

The country-of-origin principle applies to the coordinated field of law defined in Article 2. It covers only matters that are inevitably linked to taking up and pursuing the activities of an ISSP. This would be matters relating to authorisation and qualifications, the behaviour of the service provider, the quality of content, including advertising and contracts, and the liability of ISSPs. Other requirements related to the delivery of goods as such and to services provided offline are excluded.[435] Recital 21 provides an explanation of this exclusion by making it clear that the scope of the coordinated field relates to the online activities of ISSPs. It underlines this delineation with a list of excluded requirements relating to tangible goods. This includes safety standards, labelling obligations, liability for goods and requirements relating to the delivery or the transport of goods, including the distribution of medicinal products. By drawing this line, the EU appears to have been alert to the risk that rules set for online service providers could eventually pervade areas outside the scope of the ECD. This could be the case for business services that feature an electronic component, but whose substance is governed by rules to which the EU Treaties allocate a different level of competency.

The *Ker-Optika* case is a good example for the dangers that the EU perceived from blurring the functional scope of ISSPs and the boundaries of the coordinated field.[436] The CJEU ruled that a national provision which prohibited the sale of contact lenses via the internet due to public health concerns was invalid. It distinguished provisions covering the *sale* of contact lenses via the internet from those that governed the *supply* of these products. The former activity was clearly under the remit of the ECD's coordinated field while the latter fell outside its scope.[437] Restricting the online sale of these goods in order to safeguard the legitimate public health interests relating to the supply was deemed disproportionate.

It should be kept in mind that the ECD was drafted in the late 1990s and that legislators, like most other people, were unlikely to predict the emergence of platforms such as *Facebook, YouTube, Airbnb* or video-on-demand services such as *Netflix*.

---

434 Büllesbach (n 51) 306.
435 Directive 2000/31 (ECD) Article 2 (h) (i) (ii).
436 *Ker-Optika bt v ÀNTSZ Dél-dunántúli Regionális Intézete,* C-108/09 [2010] EU:C:2010:725 (CJEU)
437 ibid 23–30.

However, as e-commerce and the online platform economy have been evolving, further conflicts are programmed. Beyond the iterations of the CJEU in defining the status of newer sharing economy platforms like *Uber*[438] and *Airbnb*,[439] challenges may also arise in the area of product and intermediary liability. A clear delineation of on- and offline activities, it seems, may become more difficult in the future in view of the fact that e-commerce increasingly happens via online marketplaces and platforms whose true involvement in the transaction is not clear.[440] For example, the strict circumscription of the coordinated field to online activities leads to the situation that mandatory product labelling requirements for products sold online would be excluded, while the display of product labels in online advertising would not.[441]

Moreover, over recent years EU consumer and product law have been adapted in several areas to include, e.g. new labelling rules for online sales[442] or the classification of online marketplaces as professional traders.[443] This trend is likely to blur the borders between on- and offline rules even further.

b. The liability (exemptions) of intermediaries

The liability of intermediaries is addressed in Section 4, Articles 12 – 15 of the ECD. The 1996 Communication on Illegal and Harmful content on the internet had still favoured an industry-led, auto-regulatory approach. By late 1998 this had changed. For one, it did not appear that the emerging intermediary sector managed to come up with its own rules. Secondly, and

438 *Uber* (n 208).

439 *Opinion of Advocate General Szpunar on YA, AIRBNB Ireland UC, Hotelière Turenne SAS, Association pour un hébergement et un tourisme professionnel (AHTOP), Valhotel, C-390/18* [2019] ECLI:EU:C:2019:336 (CJEU).

440 European Commission, 'UCP Directive Guidance' (n 57) 122–127.

441 Rowland, Kohl and Charlesworth (n 128) 269.

442 For example, the Energy-labelling and Toys Safety Directives require that specific product information (warnings, energy efficiency classification) is made visible to consumers, which includes online sales: Regulation (EU) 2017/1369 of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU 2017 (OJ L 198) Article 5 (1) (a); Directive 2009/48/EC of 18 June 2009 on the safety of toys 2009 (OJ L 170) Article 11 (2); European Commission, 'Toy Safety Directive 2009/48/EC - An Explanatory Guidance Document Ref. Ares(2016)1594457' 42–43.

443 European Commission, 'UCP Directive Guidance' (n 57) 122–123.

as has been shown earlier, contradictory rulings by EU Member States' courts, including diverging interpretations of whether and how intermediaries should be made liable for third party content, had emerged over the second half of the 1990s. Thirdly, with the CDA (1996) and the DMCA (1998), the US had charged ahead with two key acts that regulated the liability exemptions of intermediaries .

Contrary to the US' sectoral approach, the EU chose a horizontal framework to regulate the liability protections of online intermediaries. It applies to all information society services (ISSPs) that act as intermediary service providers (ISPs). This latter term is, however, not clarified by the ECD. Instead, the EU creates three separate types of ISPs, which are defined through Articles 12 – 14 of the ECD.

It should be underlined that the intermediary liability regime introduced though the ECD favours a fault-based, secondary liability regime, that relies on negligence[444] and is outside of the remit of contractual liability. In fact, the ECD expressly excludes laws that apply to contractual obligations relating to consumer contracts.[445] However, the negligence bar, as will be seen, is substantial, affording intermediaries comfortable protections against liability.

Mere conduits

The first type of intermediaries are "mere conduits" of information, specified in Article 12 (1). Mere conduits relay information via a communication network or provide access to it. They would typically be the IAPs that provide individuals with an internet connection. A mere conduit would need to fulfil three conditions in order to be exempted from liability for the content it transmits. Mere conduits must not: initiate the transmission, select its receiver and select or modify the information contained in the transmission.

Article 12 (2) provides further clarification by specifying that this activity includes the transient storage of information where that storage takes place entirely as part of the transmission process. This means the information may not be kept for longer than reasonably necessary for the transmis-

444 Giancarlo Frosio and Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' [2019] Center for International Intellectual Property Studies Research Paper No. 2019-05 29, 4–6.

445 Directive 2000/31 (ECD) Recital 55.

sion.[446] Where content is being modified this must happen purely out of technical necessity during the transmission process.

The above means in essence, that a mere conduit is understood as not being an editor of the information it transmits. According to Recital 42, it needs to acts in a purely technical, automatic and passive nature[447] in order to avail itself of any content responsibility. In other words, by the same Recital, the conduit does not have either control or knowledge of the information transmitted.

These liability exemptions do not preclude courts or authorities of Member States to issue injunctions, such as in the form of orders aimed at terminating or preventing an infringement. Recital 45 specifies that these orders can be injunctions aimed at any infringement and that they include the removal and the disabling of access. Again, failure to respond to such orders would result in liability. In the area of the internet and mass communication, the intervention of the mere conduit or IAP is technically the most straightforward and, arguably, easiest way for an authority or court to interfere with the communication. Given that the conduit acts more like a neutral carrier, similar to a parcel or postal service, the justifications for marshalling the support of the IAP are likely to be justified by the cheapest cost avoider rationale rather than moral principles. As will be seen later on, there have been numerous cases in which courts and authorities have been seeking to enlist the services of IAPs to remove, stop and prevent unlawful content and activity.

The IAP landscape has also undergone diversification since the early days of the internet. With the spread of wireless internet and portable devices, new mere conduits have emerged. Wi-Fi access providers and wireless telecommunication service providers are IAPs in their own right. Public Wi-Fi networks are a feature of everyday life. These services are run by all kinds of businesses, from retailers, restaurants or coffee shops, hospitals, schools and universities, airports and transportation services to public authorities. This poses additional enforcement challenges also in this area.[448]

Caching

Caching is the process of automatic, intermediate and temporary storage of information as it travels the internet. This act is not restricted to specific services or part of a business model. Rather it is an essential technical activ-

446 ibid Article 12 (2).
447 ibid Recital 42.
448 *Mc Fadden* (n 139).

ity that aims at economising data traffic. Data packets are copied and forwarded at various connection points of the internet. At the end points of a communication, copies of popular web pages are often stored longer than needed for the actual transmission processes. They can then be called up when requested repeatedly so as to reduce data traffic on the network. The storage done through caching is therefore essentially the same as the transient storage covered under Article 12 (2), just that the storage is prolonged for the reasons explained. This provision was drawn up to protect the users and providers at the end points of a communication from being found liable for temporarily stored, cached content on their devices.[449]

In order to qualify for the liability exemptions attached to cached content the provider must meet five conditions:[450] They must a) not modify the cached content, b) comply with conditions on access to the information. This can be understood as meaning that, for example, if the cached content is paid content, the provider may not unduly access it or derive money from it. In addition, c) the information must be regularly updated according to industry standards, d) the provider must not interfere with technology that measures the use of the information (i.e. web statistics) and e) they will need to remove or disable access to cached content as soon as they gain knowledge of the fact that the source information was removed due to a court or authority order. This is meant to prevent that unauthorised content remains on the internet in the form of cached copies.

Courts or authorities may impose injunctions to require caching intermediaries to terminate or prevent an infringement.[451] In practice, this provision has however not posed any significant problems.

Hosting services

Article 14 defines hosting services as intermediaries that store information provided by a recipient of the service. The latter is the third party, such as for example a content uploader, advertiser or seller, that uses the hosting providers' service in order to post, share or sell content, service or product offers. The difference to the other two categories of intermediaries is that the storage that is provided by hosting services constitutes the actual service. The duration of the storage is decided by the third party, the recipient

449 Arno R Lodder and Andrew D Murray (eds), *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing 2017) 49.
450 Directive 2000/31 (ECD) Article 13 (1) (a) - (e).
451 ibid Article 13 (2).

of the service, and therefore not transient. The hosting service relies therefore on the recipient using an IAP to access the internet in the first place.[452]

In line with this deeper involvement, the bar for a full exemption from liability is higher than for IAPs and caching services. For this threshold to be met the following two conditions have to be fulfilled:

> *"a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*
> *b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information"*[453]

Failure to meet these requirements would imply negligence on the part of the intermediary and confer liability. This liabilityw is broad and horizontal. It can be evoked by the legal provisions that govern the illegal information and activity that the intermediary failed to act upon, be it copyright or trademark violations, IP infringements, unfair commercial practices, hate speech or other illegal content, or unfair competition.[454]

According to Article 14 (2) the hosting services provider is not eligible for the liability exemptions if it exerts authority or control over the recipient of the service, i.e. the party that requests the storage.

Article 14 (1) and (2) address therefore the two most prominent criteria for secondary liability: knowledge and control. Actual knowledge implies all liabilities, including criminal, while awareness of facts and circumstances confers civil liability.[455]

While courts and national authorities may impose injunctions to terminate or prevent infringements, like for conduits and caching services, Member States also have powers to establish procedures for information hosts that lay out how illegal content must be removed or made inaccessible.[456]

Hosting services make up a large variety of intermediaries today. This includes search engines, social media and UGC platforms, online marketplaces and cloud services, which have all been classified as hosting services on numerous occasions at Member State and EU level. This is a far cry

452 Büllesbach (n 51) 331.
453 Directive 2000/31 (ECD) Article 14 (1) (a) - (b).
454 Van Eecke and Truyens (n 316) 9.
455 Rowland, Kohl and Charlesworth (n 128) 86; Lodder and Murray (n 448) 50.
456 Directive 2000/31 (ECD) Article 14 (3).

from the more monochrome intermediary landscape from before the turn of the millennium, when IAPs, some of them hosting their newsrooms, a limited number of search engines, or the very first e-commerce marketplaces, such as eBay, ruled the scene.

No monitoring obligation

Article 15 (1) limits the possibility of Member States to oblige intermediary service providers to terminate or prevent infringements. When requiring intermediaries to prevent infringements, Member States must ensure that this is not done in a way that would oblige the service provider to monitor for illegal activity or information on a general basis or to actively search for indications of such activity. This prohibition applies to all categories of intermediaries covered by the ECD in Articles 12 – 14.

For one, this limitation is absolutely necessary for filling the neutrality condition with meaning. Were intermediaries obliged to monitor internet traffic on a general manner in order to identify and prevent illegal information, they would inevitably gain actual knowledge and acquire a degree of control that disqualifies them from immunity.[457]

Secondly, at the time when the ECD was drafted, there was a concern that more onerous obligations to proactively scrutinise the rapidly growing volume of internet traffic could pose a barrier for the development of the young internet economy.[458] A threat of liability resulting from such obligations could lead to new, innovative start-ups needing to invest undue amounts of resources into the prevention and removal of potentially illegal information. This view is supported by the EU's first implementation report of the ECD of 2003. Recognising the unsatisfactory state of filtering technology at the time, Article 15 was to protect internet intermediaries against being required to manually checking potentially millions of websites, which would pose a disproportionately high burden.

Thirdly, the 2003 report also mentions that an obligation to monitor for illegal activity and information on a general basis would result in the removal of legal content and therefore come into conflict with freedom of speech.[459] In addition, this kind of obligation could also lead to an undue

457 Büllesbach (n 51) 333.

458 *Savin*, EU Internet Law, p. 161-162.

459 European Commission, 'First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market' (2003) COM(2003) 702 final 14 fn 73.

interference with the fundamental right to privacy.[460] This would be the case if an intermediary needed to identify data of users that uploaded content, such as IP, email addresses, or user names, as part of its general monitoring efforts. Later case law at EU level underlined the role of Article 15 (1) as a safeguard for these fundamental rights.[461]

The scope of Article 15 (1)'s limiting capacity *vis-à-vis* the power of courts and authorities to impose injunctions in order to prevent specific infringements[462] has been another controversially debated feature of the ECD's liability framework.[463] From a legal point of view the controversy concentrated on the reach of specific, preventive injunctions that were effective while remaining proportional in the sense required by Article 15 (1).[464] On a more technical level, the argument turned around finding measures, such as filtering systems, that responded to injunctions targeted at preventing a particular type of illegal activity or information but did not result in the entire web traffic needing to be monitored by the intermediary.[465]

Art. 15 (2) ECD imposes two additional obligations on intermediaries. Member States may provide that public authorities be informed by intermediaries of illegal activities. In addition, the latter can be forced by authorities to provide them with the identity of service recipients with whom they have concluded service agreements. This passage was clarified by the CJEU in *Promusicae*. According to the CJEU, Member States need to balance fundamental rights (in this case intellectual property) and privacy when they design legal frameworks that deal with the communication of users' personal data.[466]

460 *Büllesbach (ed.)*, Concise European IT Law, p. 333.

461 Particularly in *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, C-360/10* [2012] EU:C:2012:85 (CJEU); and *Scarlet Extended* (n 133).

462 As provided for in Recital 47 ECD.

463 Commission, SEC(2011) 1641 Final, supra (fn. 11) para. 47–51.

464 *L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd and others, C-324/09 [2011] EU:C:2011:474 (CJEU) para. 141; Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18 [2019] CJEU EU:C:2019:821 paras 41 - 46*

465 *Nolte/Wimmers*, in: GRUR 16(2014), p. 16, 21-23; *Valcke/Kuczerawy/Ombelet*, Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common, p. 11.

466 *Promusicae* (n 140) paras 65–68.

3. Comparing the EU and US intermediary liability frameworks

The EU framework was clearly inspired by earlier US efforts. Articles 12 – 15 ECD draw from both the CDA and the DMCA. The division into functional types of intermediaries is obviously borrowed from the DMCA.[467] Nevertheless, the ECD does not provide a separate classification for search engines, which has caused separate problems due to the unique function and nature of these intermediaries. This will be discussed in more detailed in this chapter, but also, as relevant, in the sectoral analysis of Chapter 4. The knowledge standard that defined the availability of immunities in the ECD for information hosts (Article 14 (1)) is virtually identical to that of the DMCA for information hosts and search engines.[468] Both frameworks are essentially based on utilitarian arguments that favoured wide immunities out of concerns over the viability of new intermediaries' business models and the promotion of new economic actors and innovation.[469]

However, the ECD also offers important differences to the US system. The ECD's intermediary liability provisions are generally considered more rigid than those of the US.[470] The EU applies the stricter conditions of liability immunities used in the US under the DMCA for copyright violations to all content areas. There are also some specific procedural options that are absent from some or all of the sectoral pieces in the US. For example, the CDA does not provide for any court orders or injunctions targeted at preventing infringements,[471] nor does it give authorities the option to oblige online intermediaries to provide information on illegal activity or the identity of service recipients.[472] EU Member States may define reason-

467 17 U.S.C. § 512 (a) - (d).
468 ibid.
469 Koenig and Rustad (n 291) 148–149; Marcelo Thompson, 'Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries' (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 783, 786–787; Giancarlo F Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2018) 26 International Journal of Law and Information Technology 1, 32. This is also evident from the CDA in 47 USC § 230 (b) (1) - (2), the ECD, in Recital 2, and the policy document that sets out the motivations for the ECD liability framework: European Commission, 'Communication from the Commission: Illegal and Harmful Content on the Internet, COM(96) 487 Final' (n 420) 7.
470 Savin (n 384) 148; Rowland, Kohl and Charlesworth (n 128) 93.
471 Directive 2000/31 (ECD) Articles 13 (2) & 14 (3) .
472 ibid Article 15 (2).

able duties of care for intermediaries, which is an option that is not explicitly provided for in the US.

At the same time the ECD is also less specific.[473] For example, there are no detailed provisions on formats and procedures for notice requests and for counterclaims, such as those available under the DMCA).[474] Instead, these procedures are left to Member States to regulate according to their national laws.[475] The ECD also does not offer any protections for "Good Samaritans" that voluntarily engage in identifying and removing illegal content.

These differences may be explained by three reasons:

1) The more rigid EU approach towards intermediary liability is in line with an overall more interventionist stance when it comes to regulating economic actors. It should be kept in mind that in the drafting phase of the ECD varying national views on intermediary liability had to be accommodated. Different opinions on the meaning of "actual knowledge", the preventive obligations of intermediaries and the cooperation with authorities, as well as how far the remit of the EU went in prescribing liability conditions and expressing itself on sanctions, had to be reconciled.[476]
2) The lack of detail may be explained by the constitutional set up of the EU. The ECD needs to comply with the principle of subsidiarity. In areas where the EU has no exclusive competency, its remit is therefore limited to measures where Union level intervention would be more effective.[477] The ECD operates in the area of shared competency with the Member States. Consequently, it harmonises only in areas where it is absolutely necessary for the smooth operation of the internal market.
   The failure to spell out more detailed notice requirements and to formulate sanctions can arguably be attributed to this minimum harmonisation approach.[478] In addition, and as stated above, secondary liability systems are deeply rooted in the legal traditions of civil and private law

473 Edwards, 'The Fall and Rise Of Intermediary Liability Online' (n 119) 74.
474 17 U.S.C. § 512 (c) (3) & (g) (3).
475 Directive 2000/31 (ECD) Article 14 (3).
476 European Union Council, 'Progress Report - E-Commerce Directive - 8891/99' (1999) 150–153.
477 Treaty on European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2016) 2016 Article 5 para 3.
478 Büllesbach (n 51) 295. Van Eecke and Truyens (n 316) 41 fn 227.

systems within Member States.[479] Further harmonisation would have impinged on the competencies of Member States to regulate in civil criminal matters concerning defamation[480] or hate speech.[481] Areas such as copyright fall under shared competency. They limit EU intervention to aspects that concern commercial and internal market matters only.[482]

Any sectoral intervention related to unlawful content on the internet and intermediary liability at EU level would therefore need to be restricted to areas where the EU has at least shared competency. The ECD thus takes the function of a framework directive as regards intermediary lability protections and the activities of ISSPs at the content layer in general.[483]

3) Finally, it can be added that the EU wanted to ensure that its framework plugged into global efforts to regulate the internet and the information society. Recital 60 states the need for simple and clear rules that are consistent with international efforts in order to avoid EU companies being placed at a competitive disadvantage.[484] This Recital can also serve as proof and explanation for why the ECD was influenced so clearly by the DMCA and the CDA.[485]

---

479 Dinwoodie (n 312) 484; Benabou (n 334) 468–469.

480 Savin (n 384) 126–30; 'Out of Balance - Defamation Law in the European Union: A Comparative Overview for Journalists, Civil Society and Policymakers' <http://legaldb.freemedia.at/wp-content/uploads/2015/05/IPI-OutofBalance-Final-Jan2015.pdf> accessed 3 December 2020.

481 Jon Garland and Neil Chakraborti, 'Divided by a Common Concept? Assessing the Implications of Different Conceptualizations of Hate Crime in the European Union' (2012) 9 European Journal of Criminology 38, 43–47.

482 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 118 & 207. Matthias Cornils, 'Designing Platform Governance: A Normative Perspective on Needs, Strategies, and Tools to Regulate Intermediaries' (Algorithm Watch 2020) 16–20, 80–82.

483 Andrej Savin, 'Regulating Internet Platforms in the EU - The Emergence of the "Level Playing Field"' (2018) 34 Computer Law & Security Review 1215, 1223.

484 Directive 2000/31 (ECD) Recitals 58 - 60.

485 Sophie Stalla-Bourdillon, 'Sometimes One Is Not Enough! Securing Freedom of Expression, Encouraging Private Regulation, or Subsidizing Internet Intermediaries or All Three at the Same Time: The Dilemma of Internet Intermediaries' Liability' (2012) 7 Journal of International Commercial Law and Technology 22, 157.

4. Other jurisdictions

In the following a brief overview of a number of intermediary liability regimes elsewhere in the world will be given. Legislators around the world have been facing similar challenges, and borrowed from each other's frameworks, when adopting intermediary liability rules. The US and EU have served as the most common reference points for regulation elsewhere in the world.

However, the examples also show that there are notable differences and nuances when it comes to evaluating the roles of internet intermediaries and their responsibilities. These differences may be due to a variety of factors, such as specific legal and socio-cultural traditions, institutional set-ups or economic policy priorities. It should be added that the examples below relate solely to regulatory frameworks and, to some extent, court decisions . They do not provide any detail on the nature of regulatory cooperation between government and industry and the use of regulatory tools, such as self- or co-regulation.

I. Australia

Australia introduced general horizontal liability exemption rules for online intermediaries in 1999 by amending its Broadcasting Services Act of 1992. According to this, internet hosts and internet service providers will not be liable for content hosted or transmitted by them if they have not been aware of its nature. Furthermore, these intermediaries are protected from any obligation that would require them to monitor, enquire about or keep records of content hosted or transmitted.[486] The minister in charge may provide for exemptions to these rules by legislative acts. These general rules go even beyond the simplicity and broad protections offered by the US' CDA. However, the fuzziness of the requirement of "awareness" as opposed to the legally more tried and tested, although also still fluid, concept of "(actual) knowledge" as a condition for finding liability has been criticised.[487] Commentators think that beyond the rather clear act of being put on notice by a third party, the protections for intermediaries could range

486 Broadcasting Services Act 1992 Schedule 5, Clause 91.

487 Peter Leonard, 'Safe Harbors in Choppy Waters Building a Sensible Approach to Liability of Internet Intermediaries in Australia.' (2010) 3 Journal of International Entertainment & Media Law 221.

from extremely weak to very strong. In the former case, awareness would include knowledge of the mere possibility that hosted material was unlawful. In the latter, it would just cover cases of actual knowledge of the unlawful nature of specific information.[488] The absence of any safe harbour protections or notice-and-takedown obligations only adds to this ambiguity.

The rules were originally conceived with regards to objectionable content on the internet. However, their applicability to all kinds of content and related offences has been established through Australian case law. The degree of active involvement of the intermediary seems to be a common departure point for courts in determining (the degree of) awareness that would eventually lead to liability according to the very general provisions in the Australian Broadcasting Services Act.[489] However, based on the specific precedence and doctrine which developed for various torts under Australia's common law system, courts have developed different tests. As a result, a diverging and quite heterogeneous landscape of intermediary liability has emerged which applies different standard according to the legal area and violation concerned.[490]

On the one hand, an overarching impression of uncertainty and even incoherence may arise when looking at the Australian intermediary liability framework. On the other hand, this crowded landscape may reflect the diversity of the intermediary scene and the types of torts that are characteristic for content regulation on the internet. The heterogeneity may as well reflect a legal system that adapts to the reality.

Australia adapted its copyright law in 2000 to provide for instances where a carrier provides facilities that are used by another person for copyright protected acts. In such circumstances the carrier cannot be seen to "authorise" such acts.[491] However, the practical significance of this provision has been questioned as well.[492]

More recently, the Australian Government introduced legislation that obliges online platforms to report and remove "abhorrent violent materi-

488 ibid.

489 Kylie Pappalardo and Nicolas Suzor, 'The Liability of Australian Online Intermediaries' (2018) 40 Sydney Law Review 31, 485.

490 For a detailed account see: Pappalardo and Suzor (n 488).

491 Communications, 'Copyright Amendment (Digital Agenda) Act 2000' <https://www.legislation.gov.au/Details/C2004A00702/Html/Text, accessed 3 January 2020 ss 39B, 112E, and also ss 36 (1A), 101 (!a).

492 'Copyright Act 1968 (Cth) | Wilmap' <https://wilmap.law.stanford.edu/entries/copyright-act-1968-cth> accessed 3 January 2020.

al" expeditiously once they have become aware of it. This law has an extraterritorial reach in that it applies to all intermediaries globally that make material available for access in Australia.[493] The law was put in place following the live transmission of the terrorist attacks in Christchurch, New Zealand, on the social media platform *Facebook Live* in March 2019.

II. Canada

Canada stands somewhat apart from the EU and the US in that it has no statutes in place that deal specifically with the liability (exemptions) of online intermediaries. Being a common law jurisdiction, with a notable exception for the Province of Quebec, rules have developed largely out of case law, borrowing heavily from precedence that relies on cases concerning distributors in the offline world.[494] They are combined with specific common law rules related to defamation and libel.[495] Like in other jurisdictions around the world, Canadian and provincial courts have applied the concepts of (actual) knowledge, negligence and control found in secondary liability theory. For example, in *Crookes v. Newton* the Supreme Court of Canada established without difficulty that the posting of hyperlinks on an intermediary's server did not constitute an act of publication on behalf of the intermediary.[496] Even more, this ruling has been construed as meaning that there are intermediary acts (on the internet) that are so passive that immunity exists no matter whether knowledge of the illegality of the act exists or not.[497]

---

493 'Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019' <https://www.legislation.gov.au/Details/C2019A00038/Html/Text, http://www.legislation.gov.au/Details/C2019A00038> accessed 3 January 2020; Australian Government, Attorney-General's Department, 'Sharing of Abhorrent Violent Material Act - Fact Sheet' <https://www.ag.gov.au/Crime/federal-offenders/Documents/AVM-Fact-Sheet.pdf> accessed 3 January 2020.

494 Corey Omer, 'Intermediary Liability for Harmful Speech: Lessons from Abroad' 28 Harvard Journal of Law & Technology 37, 305.

495 Emily Laidlaw, 'Notice-and-Notice-Plus: A Canadian Perspective Beyond the Liability and Immunity' in Giancarlo F Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press 2019) 3–5 <https://ssrn.com/abstract=3311659> accessed 6 August 2019.

496 *Crookes v Newton* [2011] Supreme Court of Canada 33412, 3 SCR 269; Omer (n 493) 307–308.

497 Omer (n 493) 307.

Generally speaking, the fact that a notice has been received, and how it has been processed by the intermediary, will also play a role when deciding on liabilities. Many provincial laws have specific conditions for notices. However, they rely on press law in the offline world. Their applicability to online intermediaries is not entirely clear.[498]

Only in 2012 did Canada introduce a legal framework that specifically includes provisions for intermediary liability. However, this is restricted to the area of copyright. The Copyright Modernization Act of 2012 categorises intermediaries similar to the approach in the EU into network services (i.e. IAPs), caching and hosting services.[499] Copyright owners may notify intermediaries of infringing content. Like in the US, but unlike the EU, the form and content of such notices are clearly defined by the law.[500] However, intermediaries are only obliged to forward these notices to the uploader within 30 days of receipt and keep a copy. This so-called Notice-and-Notice regime means an internet service provider is not required to judge on the request received and is also not in a position of actual knowledge regarding the content in question. It does however require search engines to delete caches of notified content that has been removed by uploaders.[501] Whether this regime would also be practical for other kinds of unlawful content, such as defamatory or terrorist speech, is a subject of discussion.[502] This supposedly light touch approach to intermediary liability is somewhat relativised by the 2017 judgement in *Equuestek*. The Canadian Supreme forced *Google* to delist search results that linked to pages of a company that infringed *Equuestek's* trademark rights on a worldwide basis.[503]

498 ibid 306.

499 Copyright Modernization Act 2012 (SC 2012, c 20) s 31.1., for more detail see: Federica Giovanella, 'Online Service Providers' Liability, Copyright Infringement, and Freedom of Expression: Could Europe Learn from Canada?' in Mariarosaria Taddeo and Luciano Floridi, *The responsibilities of online service providers* (Springer Berlin Heidelberg 2016) 234–237.

500 S.C. 2012, c. 20 s. 41.25.

501 Employment and Social Development Canada, 'Notice and Notice Regime' (*gcnws*, 17 June 2014) <https://www.canada.ca/en/news/archive/2014/06/notice-notice-regime.html> accessed 20 December 2019.

502 Laidlaw (n 494).

503 *Google Inc v Equustek Solutions Inc* [2017] Supreme Court of Canada 36602, 1 SCR 824.

III. China

China started in 2000 to introduce horizontal provisions aimed at regulating the liability protections for online intermediaries. These fairly general provisions provide that internet service providers must not reproduce, post or disseminate illegal information and stop the transmission of the information once they become aware of it.[504] Largely based on the US DMCA, they did not, however, provide for any safeguards against the possibility of imposing general monitoring obligations,[505] nor did they differentiate between different types of intermediaries. Courts applied these rather broad rules and developed them through case law, mainly in the area of defamation and copyright. As a result, a distinct fault-based regime developed, which focussed on imposing strict liability on intermediaries depending on their involvement in the act of dissemination. Courts eventually adopted a lighter approach by tying liability to the receipt of and reaction to a notice before moving to a broader knowledge-based liability. Under the latter approach Chinese courts have recently moved to finding fault with intermediaries where they "should have known" about illegal content on their servers.[506] Broadly speaking, this means the courts have looked into duties of care that can be reasonably expected of such intermediaries relating to the detection and removal of unlawful information.

In 2010, China passed a horizontally applicable Tort Liability law, which solidifies the fault–based standard for intermediary liability by taking knowledge as a yardstick.[507] China supplemented these horizontal rules with online intermediary liability provisions specifically relating to copyright. First introduced in 2000, they were last revised in 2012 in order to bring in place safe harbours and clarify that ISPs are not obliged to monitor on a general basis for infringing information.[508] The safe harbours mainly apply to ISPs that react to notices and to those that can prove that infringing information was outside of what they "should have

504 Qian Tao, 'Legal Framework of Online Intermediaries' Liability in China' (2012) 14 info 59, 59–60.

505 Jie Wang, 'Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – As Compared to the US and German Routes' (2015) 46 IIC - International Review of Intellectual Property and Competition Law 275, 278.

506 Tao (n 503) 60–62.

507 Q Tao, 'The Knowledge Standard for the Internet Intermediary Liability in China' (2012) 20 International Journal of Law and Information Technology 1, 2–3.

508 Wang (n 504) 279–280.

known" given the circumstances at hand. The Chinese law puts down a set of indicative criteria which relate to the role of the platform in the transmission process, its business model, its notice processes and its preventive activities.[509] Courts have further interpreted these criteria and applied so-called "red flag" tests, not only in copyright cases, but also in areas such as defamation or counterfeiting.

Overall, a distinctive approach has developed, which, although borrowing heavily from the US and the EU, appears to apply more qualified and onerous duty of care obligations to online platforms, which includes the use of automated preventive tools. As a result, the Chinese intermediary liability system can generally be seen as stricter than that of the US and the EU. At the same time, it may have developed more elaborate tests and methodologies on how to assess intermediaries' duty of care. However, outside the area of copyright the rather general provisions have led to courts applying homegrown approaches towards duty of care,[510] which combine doctrines from its own civil law system with that of various other jurisdictions, mainly in the US and EU.[511]

IV. India

India introduced rules for liability exemptions of internet intermediaries in Section 79 of the Information Technology Act in 2000. These rules were originally very general. They stated that network service providers shall not be liable for any third party information if they can prove that they had no knowledge of its unlawful character and applied due diligence to prevent any offences. The rules were amended in 2008 by more specific provisions that appear to be referring at least partly to the ECD. The amended section 79 now introduces a categorisation similar to Articles 12 – 14 of the ECD by exempting intermediaries that provide access to communication systems over which data is transmitted, temporally stored or hosted.[512] A passivity condition introduces the requirement that those intermediaries do not initiate, select or modify the data transmitted, or select its receiver.[513]

509 ibid 286.
510 INTA Anticounterfeiting Committee China Subcommittee, 'Online Counterfeiting Issues and Enforcement in China (CT20)' (International Trademark Association 2015) 10
511 Tao (n 503) 60, 67.
512 Information Technology (Amendment) Act, 2008, s. 79 (2) (a).
513 ibid (2) (b).

That wording is almost identical to Article 12 (1) ECD. Importantly, however, subsection (2) (c) makes the liability exemption also dependent on due diligence obligations identified in the Act and additional guidelines that may be issued by the government. Meanwhile, the liability exemptions would not apply if the intermediary had abetted, aided or induced the unlawful acts and, upon receiving actual knowledge, did not act expeditiously to remove or disable access to that material.[514]

The Indian Government passed more detailed guidelines on the due diligence obligations of internet intermediaries in 2011.[515] These guidelines specify amongst others that online intermediaries need to publish their rules and conditions of use clearly to users and inform them of the fact that various types of unlawful information must not be communicated through their systems. Intermediaries are obliged to remove unlawful information of which they have gained actual knowledge within 36 hours. That knowledge can be obtained through notification by third parties or through the intermediary's own investigative activity. In addition, the intermediary must have in place IT security measures to protect its information and network integrity.

Despite borrowing notably from the ECD's provisions in Articles 12 – 14, the Indian intermediary liability framework has been seen as imposing more onerous obligations, and subsequent liability risks, on internet intermediaries than for example the US or the EU.[516] It relies heavily on due diligence obligations as a precondition for avoiding liabilities for passive internet intermediaries, without however distinguishing between different kinds of intermediaries.[517] In addition, the Indian laws lack any limitations on the scope of due diligence obligations, notably the kind of limitations that prohibit general monitoring obligations, such as provided in Article 15 ECD.

This more hawkish stance on internet liability *vis-à-vis* intermediaries has been confirmed in case law. For example, in *Louboutin v Bajaj*, the French trademark owner successfully sued Indian e-commerce market-

514 ibid (3).

515 Information Technology (Intermediaries Guidelines) Rules, 2011, GSR 314(E) Rule 3.

516 Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet' [2011] SSRN Electronic Journal 2–4 <http://www.ssrn.com/abstract=2038214> accessed 2 January 2020.

517 ibid 3.

place *Davey.com* for violating its trademark right.[518] The court ruled that the due diligence obligations imposed on internet intermediaries by Indian Law were broad and far-reaching. A strict word-by-word application of the law with regards to notifying and informing sellers of the inadmissibility of unlawful acts through terms and conditions was not sufficient. Given the involvement of the marketplace in the sale and transaction, the due diligence specified under Indian law would extend to enforceable contracts between seller and platform and further measures to assure the authenticity of products sold.[519] Meanwhile, the Delhi court also offered detailed criteria to determine when an online marketplace can be seen as playing an active role in the intermediation process, making it subject to enhanced due diligence requirements and reduced protections from liability.[520]

The intermediary liability conditions of the Information Technology Act and the Intermediary Guidelines, apply horizontally, with the exception of copyright. The Copyright (Amendment) Act 2012 exempts any intermediary that stores works in a transient or incidental way during the process of electronic transmission or communication to the public. Likewise, the act of providing access through links to works during such process, where not expressly forbidden by the rightsholder, shall also not constitute a violation of copyright.[521] The NTD regime requires intermediaries to disable access to content for 21 days after receipt of a written notice. Any longer lasting removal will need to be achieved through a court order. The procedural details of the notice-and-takedown regime are specified through statutory Copyright Rules.[522] They regulate the content and format of notices, reaction times and information obligations. However, they do not provide for specific counter-notice procedures.

This description of the various intermediary liability frameworks demonstrates that at the outset, many jurisdictions around the globe had chosen similar legal approaches when tackling the occurrence of unlawful content and activity on the internet. With the notable exception of Canada, many international regimes were influenced by the CDA and the DMCA, the pioneering US acts in that respect. At a closer look, the regimes

518 *Christian Louboutin Sas v Nakul Bajaj & Ors on 2 November, 2018* [2018] High Court of Delhi CS COMM - 344/2018.

519 ibid paras 70, 82; Pratik Dixit, 'Liability of Indian E-Commerce Websites for Trade Mark Infringement by Sellers' (2019) 14 Journal of Intellectual Property Law & Practice 424.

520 *Christian Louboutin Sas v Nakul Bajaj & Ors on 2 November, 2018* (n 517) para 56.

521 Copyright (Amendment) Act, 2012, s. 52 (b) (c).

522 Copyright Rules 2013, GSR 172(E) Rule 75.

portrayed here offer some important differences. *Savin* distinguishes between three intermediary liability regimes: those allocating full liability to intermediaries, an early option now abandoned by most jurisdictions across the globe; the US model of generous liability immunities, and an EU style model that ties stricter conditions to the immunity of intermediaries.[523] Moreover, the EU has favoured a horizontal model that imposes identical liability immunity conditions regardless of the type of infringement, an approach also initially embraced by Australia, China and India. The US meanwhile selected a model that allocates levels of protections by type of infringement (i.e. speech acts, copyright, trademarks).

It appears that of the frameworks discussed above, those of the US and the EU are the only ones that have stayed relatively static over the last 20 years. All other jurisdictions have seen major changes and amendments that have generally lowered the bar for intermediary liability. This trend has usually been accompanied by a sectorisation of rules, with copyright being a main target of stricter intermediary obligations. This sectoral adjustment may be relevant for current EU initiatives to reform the ECD. Notably India and China have recently emerged with more elaborate duty of care obligations, partly by weakening certain safeguards that are upheld in other jurisdictions. These newer systems and the experiences gained from their application may provide valuable insights for the EU's current efforts. Meanwhile, even the current US system has been subject to political initiatives that aim at imposing higher barriers to immunity on online intermediaries.

The section also demonstrates that over the last 10 years at least, intermediary liability rules appear to diverge on an international level, partly as a response to specific cultural, political and economic pressures,[524] and partly due to the particularities of national legal systems. The remainder of this chapter and the sectoral analysis of Chapter 4 will show that similar pressures exist within the EU.[525] Arguably, the EU, as a political and economic union, is more compelled to countering these diverging trends at

523 Savin (n 384) 146–147.

524 Thomas Poell, David Nieborg and José Van Dijck, 'Platformisation' (2019) 8 Internet Policy Review 8–9 <http://policyreview.info/node/1425> accessed 28 January 2020.

525 European Commission, 'SEC(2011) 1641 Final' (n 11) 26–20; Cornils (n 481) 76–79. Alexandre de Streel and others, *Moderation of Illegal Content Online: Law, Practices and Options for Reform.* (EU Publications Office 2020) 19 <https://data.europa.eu/doi/10.2861/831734> accessed 7 October 2020.

Member State level. Meanwhile, this makes the challenges of drafting new laws that are consistent with international rules even more difficult.

D. Enforcement challenges in internet intermediary liability

1. Emerging challenges - EU reviews of the ECD

The ECD obliged the Commission to re-evaluate its intermediary liability framework by 2003 and within a time frame of every two years thereafter. An emphasis was put on review of the need to adapt the categorisation of intermediaries and the necessity to harmonise NTD procedures.[526]

I. The 2003 and 2007 ECD evaluations

The first review of the ECD in 2003, however, found that there was no sufficient experience yet on the practical application of Articles 12–14. The few court rulings available by that time on the matter of intermediary liability had taken place prior to Member States implementing the ECD into their national laws.[527] The 2003 ECD application report also found no grounds that justified regulatory intervention in the areas of NTD and the categorisation of internet intermediaries.

In 2007, the European Commission published two reports that evaluated the implementation of the ECD and its impact. While one of these reports evaluated the economic impact of the ECD,[528] the other one, by *Verbiest et al*, specifically looked into the transposition and the practical application of the intermediary liability exemptions regime by Member States.[529] The first study found that many internet intermediaries at the time welcomed the provisions of Articles 12 -15 ECD as providing legal certainty for their business models. However, it also pointed out two areas of ambiguity. Firstly, intermediaries were unsure how far they could stretch their own voluntary preventive efforts against unlawful activity and

526 Directive 2000/31 (ECD) Article 21.
527 European Commission, 'First Report on the Application of Directive 2000/31/EC' (n 458) 13 fn 71.
528 Dr Claus Kastberg Nielsen and others, 'Study on the Economic Impact of the Electronic Commerce Directive' (DG Internal Market and Services, European Commission 2007).
529 Verbiest and others (n 315).

content. While there was no obligation to generally monitor all information, it remained unclear in how far voluntary efforts to monitor web traffic for unlawful content could lead to liabilities in cases were the intermediary detected content or missed to detect content. Secondly, this study found that legal uncertainty existed as to whether search engines were within the scope of Articles 12 – 15 ECD.[530]

Verbiest et al noted in the second study a number of emerging problems when it came to the practical application of the intermediary liability provisions by courts, particularly those concerning host providers covered by Article 14 ECD. First, the study indicated uncertainty over the terms "actual knowledge" and "aware(ness) of facts or circumstances from which the illegal activity or information is apparent", which are both conditions that determine the liability of intermediaries.[531] There was a lack of understanding over the level of knowledge required to make it "actual" knowledge. The question centred around knowledge of specific content *and* its unlawful character versus knowledge that was created from automated activity of computer software, such as databases or monitoring tools, or through negligent ignorance.[532] The conditions under which such actual knowledge or awareness could be established, varied according to definitions, specific tests and doctrines relating to knowledge and awareness in Member States' legal systems. Lastly, it was not clear when an intermediary service provider could be considered to have been put on notice and incurred liability after failing to act appropriately, as the ECD did not establish common procedural requirements in that area. These uncertainties led to a fear that intermediaries would be pressured into becoming private judges over the legality of content and speech.[533]

Furthermore, the study identified potential problems that courts had in reconciling obligations arising from injunctions aimed at preventing specific violations with the preclusions of general monitoring. The study points to specific court cases in Germany, Austria, Italy, Sweden, Belgium, the Netherlands and the UK where the permissibility and scope of so-called stay-down orders against both IAPs and host providers was controversially debated. The orders concerned unlawful content and activity in

530 Nielsen and others (n 527) 16–22.
531 Directive 2000/31 (ECD) Article 14 (1); Verbiest and others (n 315) 36–47.
532 Verbiest and others (n 315) 36–37.
533 ibid 41–42.

the areas of terrorist speech, child pornography and intellectual property law.[534]

Finally, the study noted the emergence of newer Web 2.0 intermediaries. These new types of intermediaries were referred to as content aggregators, such as video-sharing platforms and the first social media sites. The report noted the potential for legal controversy over the role of these players in the intermediation process and the availability of the liability exemptions of Article 14 ECD.[535]

Overall this study provides a comprehensive and detailed insight into how Member States' courts tried to interpret the rules laid down by Articles 12 – 15 ECD and their national implementations. The different legal traditions and doctrines, combined with different degrees of understanding of the new, technically complex and rapidly evolving intermediation models gave a glimpse of the problems that were to come.

II. The 2012 public consultation

The EU's 2012 public consultation on the application of the ECD shows that the initial frictions of 2007 had developed into fully blown legal problems: the staff working document accompanying the consultation states that "a wide variety of stakeholders face a high degree of regulatory uncertainty about the application of the intermediary liability regime of the E-Commerce Directive."[536] Apart from the issues mentioned in the 2007 study, the diverging assessments on the kind of intermediaries covered by Art. 12–14 of the ECD had moved to centre stage. By that time, new Web 2.0 intermediaries had grown into sizeable actors of the internet and information economies. Video-sharing platforms and social networks' business models increasingly relied on the commercialisation of user data. They reaped the first benefits from network effects as they emerged into multi-sided platforms. In addition, e-commerce marketplaces and collaborative economy platforms were starting to disrupt more traditional offline sectors of the economy, such as high street retail, travel, accommodation and transportation services.

The problem of unlawful content and illegal activity, meanwhile, persisted and the ECD's liability framework did not provide for an effective

534 ibid 48–71.
535 ibid 102–104.
536 European Commission, 'SEC(2011) 1641 Final' (n 11) 25.

and consistent enforcement against this. The 2012 stakeholder consultation exposed four main problem areas: 1) the definition of intermediary activities in Articles 12 to 14 ECD; 2) the conditions for the availability of the safe harbour in Articles 12 to 14 ECD; 3) the unclear and fragmented nature of NTD procedures; 4) the general monitoring prohibition in Article 15 and its relation to specific, preventive injunctions.[537] A plethora of national court rulings with diverging and even contradictive interpretations serve as a testimony to the ineffectiveness and ambiguities of the ECD's liability provisions. The matter was aggravated by differing transpositions of this Directive into national laws. More detail on this will be provided in the following section.

However, in its evaluation exercise of the E-Commerce Action Plan, the Commission followed the pleas of intermediaries and user representations, which had constituted the majority of stakeholders that had participated in this exercise, and refrained from any attempts to reform the ECD's liability framework.[538]

III. Reviews and initiatives under the Digital Single Market policy

Five years later, the Commission found that unlawful content on the internet, and on online platforms, had not just persisted but actually continued to proliferate. At the same time, it noted the ascendance of online platforms to gatekeepers, which held sway over large parts of the internet's ecosystem, governing access to information and content.[539] Further stakeholder consultations conducted in 2016 had revealed a divided opinion over the fitness of the then over 15-year-old liability framework to effectively address the problem of unlawful content in the Web 2.0 era of multisided online platforms. A synopsis report of the 2016 consultation showed that rightsholders and notice providers were largely at odds with it, citing the above voiced legal unclarities as persisting and in need of adjustment.

537 ibid 25–26.

538 European Commission, 'E-Commerce Action Plan 2012-2015, State of Play 2013, SWD(2013) 153 Final' (2013) 17.

539 European Commission, 'Communication on the on the Mid-Term Review on the Implementation of the Digital Single Market Strategy - A Connected Digital Single Market for All COM(2017) 228 Final' (2017) COM(2017) 228 final 7–8; European Commission, 'COM(2016) 288 Final' (n 223) 2.

Intermediaries themselves, user organisations and content-uploaders were largely satisfied with the provisions.[540]

In view of this divided picture the EU vowed to "maintain the existing intermediary liability regime while implementing a sectoral, problem-driven approach to regulation."[541] The Commission would focus on a review of intermediary liability responsibilities in the area of copyright and audiovisual media services.[542] It would step up efforts to encourage platforms to take more responsibility through self-regulatory measures. That sectoral focus, however, implicitly meant that the overarching horizontal liability provisions in Articles 12 – 15 ECD would remain unchanged. In the wake of the sectoral reviews in copyright and audiovisual media services a number of other sectoral initiatives sprang up or were re-enforced, which all dealt with the responsibilities of intermediaries, and hosting services in particular.[543] These initiatives will be discussed in more detail in the sectoral reviews of Chapter 4.

The Commission confirmed its sectoral approach in a 2017 Communication and a 2018 Recommendation both aimed at tackling illegal content online.[544] Both initiatives acknowledged the link between sectoral enforcement at EU level, directed at the various kinds of unlawful content, from hate speech and disinformation to intellectual property violations and illegal and unsafe products. At the same time, they affirm an emerging con-

---

540 European Commission, 'Synopsis Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy' (European Commission 2016) 15–21 <https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and> accessed 29 March 2017.

541 European Commission, 'COM(2016) 288 Final' (n 223) 9.

542 ibid.

543 'Code of Conduct on Countering Illegal Hate Speech Online' (2016) <http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf> accessed 9 March 2017; 'Memorandum of Understanding on the Online Sale of Counterfeit Goods, 2016' <http://ec.europa.eu/DocsRoom/documents/18023/attachments/1/translations/> accessed 17 March 2017; European Commission, 'Memorandum of Understanding on Online Advertising and Intellectual Property Rights' (2018) <https://ec.europa.eu/docsroom/documents/30226> accessed 26 June 2020; European Commission, 'COM(2018) 236 Final' (n 70); European Commission, 'Product Safety Pledge Voluntary Commitment of Online Marketplaces with Respect to the Safety of Non-Food Consumer Products Sold Online by Third Party Sellers' (European Commission 2018) For a summary overview see: European Commission, 'COM (2017) 555 Final' (n 69) 2–3.

544 European Commission, 'COM (2017) 555 Final' (n 69); European Commission, 'C(2018) 1177 Final' (n 8).

sensus that internet intermediaries, notably online platforms, should step up their efforts, and take on more responsibilities in the fight against unlawful content.

The articulation of enhanced responsibilities for platforms appears to have arisen out of public consultations. It took a more concrete form as stakeholders called for the definition of duties of care that internet intermediaries would need to commit to in the removal but also the prevention of unlawful content. The imposition of duties of care is, at least theoretically, an option offered by Recital 48 of the ECD.

On the side of the EU, the concept of duty of care has not been explored further. There remain different understandings of the concept of duty of care, which some stakeholders, notably intermediaries, tend to see as more voluntary commitments, often entirely targeted at *ex-post* activities in the form of NTD procedures and transparency reports. On the other side of the spectrum, damaged parties would see these duties of care extend to statutory obligations that include proactive measures aimed at identifying and preventing harms and violations.[545]

While enhanced responsibilities for internet intermediaries where increasingly discussed by the EU at least since 2016, it has remained unclear if and how they would be reconciled with the broad protections offered by the ECD.

In July 2019, the new European Commission president-elect, *Ursula von der Leyen*, announced that under her presidency in 2019 – 2024 the EU would draft a Digital Services Act (DSA) in a bid to overhaul the ECD. The aim would be to "*upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market.*"[546] A leaked note of the European Commission's Digital Single Market Strategic Group confirmed that such an Act would finally look at reforming Europe's horizontal liability framework for intermediaries.[547] Amongst others, that draft confirmed that online platforms are increasingly subject to diverging liability rules across Member States. These differing rules are partly due to diverging interpretations by national courts on the liability provisions of the ECD. This, in turn, is owed to outdated provisions of the ECD, which has

545 European Commission, 'Synopsis Report on the Regulatory Environment for Platforms' (n 539) 19–20.

546 Ursula von der Leyen, 'A Union That Strives for More - My Agenda for Europe. Political Guidelines for the next European Commission 2019 - 2024' 13.

547 The leaked note is available under 'Digital-Services-Act-Note-DG-Connect-June-2019.Pdf' <https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf> accessed 7 January 2020.

been overrun by new platform economy business models, technologies and socio-technical realities. Over the year 2020, the Commission's plans for a new DSA were further elaborated and supplemented by a public consultation. Published on 15 December 2020, the focus of the proposed DSA is on providing an enhanced set of obligations in addition to the existing intermediary liability exemptions regime of the ECD, and a specific regime for so-called large gatekeeper platforms.[548] The details of this original proposal will be evaluated briefly in the relevant sectoral sections and in Chapter 6. A more in-depth analysis has been published elsewhere since.[549] In addition, the DSA package will undoubtly be subject to intense negotiations, with further changes being made during the EU policy making process during 2021. It may only be finally adopted during 2022 or later.

IV. Main legal challenges of the ECD inhibiting enforcement against unlawful content

The EU's reviews of the framework of intermediary liability exemptions and its practical application since 2003 reflect a number of distinct problems. The EU, however, was not alone with this. More than that, these reviews were an expression of even more intense discussion on this matter in society at large, in academic, industry and civil society circles over the last 15 years. As early as 2004, *Edwards* remarked that there was a fundamental change under way in the intermediary landscape, with the emergence of content aggregators (search engines, price comparison sites) and P2P file sharing. The new roles that these intermediaries would play in the of exchange information online may lead lawmakers to substantially review existing liability rules for these players.[550] Five years later, she stated that Articles 12 – 15 of the ECD were desperately in need of review.[551] On the academic side, the debate has advanced further with a variety of proposals that aim at reforming today's intermediary liability framework to varying degrees. Many of these debates are linked to specific content areas, such as

548 European Commission, 'The Digital Services Act Package' (n 8).

549 For example: Mark D Cole, Christina Etteldorf and Carsten Ullrich, *Updating the Rules for Online Content Dissemination: Legislative Options of the European Union and the Digital Services Act Proposal* (Nomos 2021).

550 Edwards, 'The Changing Shape of Cyberlaw' (n 16) 364.

551 Edwards, 'The Fall and Rise Of Intermediary Liability Online' (n 119) 87.

hate and terrorist content, disinformation, copyright, trademarks or child abuse material. An overview of these proposals will be given in Chapter 6.

To summarise, a number of vectors can be identified that have contributed to challenging the original intermediary liability provisions of the ECD, but also other intermediary liability frameworks around the world:

a) technological advances: the rise of Web 2.0 interactivity, mobile internet, technology convergence, data storage and connection capacity;
b) business innovation: big data exploitation, e-commerce, collaborative economy platforms, online streaming, user-generated content platforms;
c) user behaviour: growth in internet use across the world population and by time spent per user on the internet;
d) socio-economic importance of internet intermediaries: indispensable for the operation of the internet (content and infrastructure gatekeepers), enablers of information exchange/speech conduits, amongst the most valuable and powerful corporations worldwide.

These tendencies are interconnected: for example, technological advances in data storage, bandwidth or wireless applications directly impact business models and user behaviour.

Three main problem areas have crystallised out of the plethora of legal issues that have been generated by the above changes.[552]

1) the neutrality/passivity condition for non-liable online intermediaries;
2) the meaning of actual knowledge;
3) the preventive obligations of intermediaries.

These three problems will be analysed in more detail in the following section. The analysis shall first serve as a basis for developing a deeper understanding of underlying legal and technological factors that shape consider-

552 The following publications shall serve as examples for more detailed discussions of these problems: Zuboff (n 5) ll 1997–2050; Rowland, Kohl and Charlesworth (n 128) 85–92; Martens (n 53) 33–35; Peggy Valcke, Aleksandra Kuczerawy and Pieter-Jan Ombelet, 'Did the Romans Get It Right? What Delfi, Google, EBay, and UPC TeleKabel Wien Have in Common' in Mariarosaria Taddeo and Luciano Floridi, *The responsibilities of online service providers* (Springer Berlin Heidelberg 2017) 11–16; Georg Nolte and Jörg Wimmers, 'Wer Stört? Gedanken Zur Haftung von Intermediären Im Internet – von Praktischer Konkordanz, Richtigen Anreizen Und Offenen Fragen' (2014) 16 GRUR.

ations over internet intermediary liability today. Secondly, it demonstrates the challenges of enforcing against unlawful content on the internet in an exemplary manner. Finally, it shall also be useful when discussing options for alternative regulatory frameworks in the last chapter.

The analysis below also highlights the multi-dimensional and multi-layered nature of the problems at hand. Should a legal analysis of the enforcement problems be approached by looking at the different categories or business models of intermediaries, or should it start from the type of infringement, violation or harm at hand, i.e. defamation, terrorist content, copyright. Certain types of unlawful content have typically been connected with specific types of intermediaries: defamation with social networks, trademark infringements and product safety with e-commerce marketplaces, copyright with UGC platforms, hate speech with social media and UGC platforms. Search engines may be the only type of intermediary where almost all types of infringement would be apparent. In Chapter 4, each legal challenge will be analysed according to how it played out in case law. The CJEU's mixed success in providing clarification will also be discussed.

It should be mentioned that these problems are not restricted to the EU. Legal systems across the world have had to grapple with essentially the same questions when it comes to unlawful content online. With that in mind, the following detailed analysis of the main challenges of the ECD's liability framework will be supplemented with case law from jurisdictions outside the EU where this helps to illustrate possible alternative approaches.

2. ECD intermediary liability – the main challenges through case law

The availability of the hosting defence had originally been discussed mainly in light of the intermediary business models in questions. Courts' assessments of the active or passive role was necessarily tied to the activity of the intermediary and the kind of content hosted – be it product offers, news and comments, or entertainment. Therefore, the analysis of the first challenge, determining the neutral status of intermediaries, will be done from the angle of different intermediary business models.

Once courts established that intermediaries qualified for the liability exemptions of the ECD, they applied the specific conditions of that regime. Actual knowledge of unlawful information or activity is one central condition for liability. However, courts have had marked difficulties in interpreting this requirement in a consistent fashion throughout the EU.

Where intermediaries are found to have actual knowledge of illegal content or activity, they are obliged to remove or disable access to it. Very quickly, however, the Sisyphean task of purely reactive blocking and removal of illegal content on the internet became clear. Rightsowners and damaged parties made use of the option given under the ECD to apply for preventive injunctions of already notified violations. Soon, the scope of these preventive injunctions broadened and hit the limitations imposed by Article 15 ECD that prohibits the imposition of general monitoring duties. This conflict is a technical as well as a legal one and shall be discussed as the third legal challenge of the ECD.

I. The neutrality of internet intermediaries

The premise that intermediary actors with no knowledge or control over third parties and their actions are free from liability for these acts is a basic concept of secondary liability. By contrast, secondary liability may be attributed when those intermediaries are found to play a more active part in the intermediation process, which would imply an involvement that confers a certain level of control and/or knowledge. Neutrality, or passivity, is therefore a precondition for the availability of the liability exemptions under the ECD. Recital 42 refers to the "*mere technical, automatic and passive role*" of intermediaries and Articles 12 (1), 13 (1) and 14 (1) provide the basis of this principle.

Establishing the (degree of) passivity or neutrality of intermediaries is a central test that courts in the EU have applied in order to decide whether the liability immunities of the ECD are available. In the two extreme scenarios a provider is either so actively involved in the intermediation process that they would be considered an editor or publisher of information, which could even lead to conferring primary liability. On the other hand, a totally neutral host would be assessed with regards to compliance with the conditions set out under Articles 12 – 14 in order to qualify for the exemptions from intermediary liability.

During the first years of the ECD there seemed to be little controversy for courts in deciding on the availability of the immunity protections for intermediaries. The type of business models in the focus of litigation were IAPs, blog portals or P2P file sharing networks. Mere conduits or IAPs have, in general, never had to fear that the protection of the ECD would not be available to them. The controversies in the application of the ECD relate mainly to internet hosts and can be linked to the rise of new types of

Web 2.0 intermediaries, such as information location tools (search engines), UGC or social media platforms, and e-commerce marketplaces.[553]

a. Search engines

Unlike in the US intermediary liability provisions, the ECD does not offer a separate classification for search engines. National courts came therefore initially to diverging outcomes when considering the categorisation of internet search engines. Courts in Germany, UK, Belgium and France classed these actors respectively as information hosts (Article 14 ECD),[554] mere conduits (Article 12)[555] or as editors and therefore not eligible for the protections of the ECD.[556]

These divergences were eventually put to bed by the CJEU ruling in *Google France,* which established criteria according to which a search engine could be considered an active or passive host.[557] The rightsholders of the French luxury product group *LVMH* claimed that *Google* asserted control over the content of its web search results by assisting clients in using the AdWords service: *Google* drafted the commercial text next to the ad link and suggested keyword combinations to ameliorate the effectiveness of the displayed adverts. Those ads were displayed in the form of "sponsored links" that led to websites that offered fakes of products, for which *LVMH* enjoyed trademark protection.

The highest EU court ruled that a search engine operator, whose search engine matched user requests with keywords or a combination of keywords selected by advertisers, which then led to search results being displayed, did not play an active role. By contrast, where the operator created the advertising message that appeared next to sponsored links and assisted in the selection of the advertising keywords to improve the relevance of the sponsored links, this may indicate such an active role and lead to a de-

553 European Commission, 'SEC(2011) 1641 Final' (n 11) 26–30; Waisman and Hevia (n 313) 797–800.

554 *Vorschaubilder* [2010] BGH I ZR 69/08, MMR 2010 475; *Jean-Yves Lafesse et autres v Google et autres* (2009) (Unreported) (Tribunal de grande instance de Paris, 3ème chambre).

555 *R v Rock and Overton,* [2010] Gloucester Crown Court T20097013,

556 *Copiepresse et al v Google Inc* [2007] Brussels Court of First Instance 7964. For more detail on these cases see: European Commission, 'SEC(2011) 1641 Final' (n 11) 27.

557 *Google France v Louis Vuitton* (n 155) para 143.

nial of the classification as a hosting service under Article 14 ECD.[558] The outcome did confirm that search engines, when they remain passive, would be classified as host providers under the ECD. However, it did not solve the problem of the general availability of the hosting defence for search engines, because the CJEU said that national courts would need to assess based on the concrete facts at hand whether the criteria it had laid down as guidance did indeed apply.

The guidance delivered by the CJEU translated into largely favourable rulings for *Google's* search engine operations. Judges either accorded the hosting privileges or tried to circumvent the tricky questions of deciding on the active role of the search engine.[559] However, some courts still found *Google's* search engine as too active for deserving the host status of the ECD, in particular when looking at the company's *Autocomplete* or *Suggest* functionality.[560] Today, many of the large e-commerce or social media platforms, such as *Amazon* or *Facebook* own search engines in their own right. For these search engines, questions of liability have been assimilated into the hosting liability of the platform into which they are integrated.[561]

b. E-commerce marketplaces

i. National case law

E-commerce marketplaces belonged to the first intermediaries that started to affect the real economy in a sense that they competed directly with traditional brick and mortar high street retailers. While providing access to millions of products at an international level, they also acted as product search engines, utilising data from clients, customers and sellers alike for personalised advertising and expansion into adjacent markets.[562]

---

558 ibid 115–119.

559 Jacques Larrieu, Christian Le Stanc and Pascale Tréfigny-Goy, 'Droit Du Numérique Juillet 2010 - Août 2011' Recueil Dalloz 2011 2363.

560 *Google France c/ Syndicat Français de la Literie* (2010) (Unreported) (Cour d'appel de Paris Pôle 5); *Olivier M c/ Prisma Presse, Google* (2011) (Unreported) (Tribunal de Grande instance, Paris, 17eme chambre).

561 See for example *Cosmetic Warriors Ltd & Anor v amazon.co.uk Ltd & Anor* (2014) [2014] EWHC 181 (Ch).

562 *Amazon*, for example, is known for its aggressive expansion into private label products, logistics and web hosting services, payment, product insurance and consumer credit services. These services benefit from competitive intelligence

Early cases against marketplaces mainly focussed on *eBay*. In France, courts have held *eBay's* activities as consisting of hosting, publishing and of brokering. In 2008, *eBay* was found by a Paris court to provide its sellers with tools to set up their own stores and promotional activity, send commercial reminders and run a "Power Seller" program. These activities were all geared towards increasing sales and subsequently *eBay's* commissions. This conferred on it a "very active" role within the sales process. In line with its active involvement, *eBay* had a general obligation of supervision to prevent the sales of obviously counterfeit products, which took place on a massive scale. It could not benefit from the hosting defence for merely technical service providers under the ECD. The court also defined some of these preventive measures, such as for example verifying the identity of sellers and requiring sellers to prove the authenticity of their products.[563] This view was shared by the *Tribunale de Grande Instance de Troyes* in *Hermès International v Feitz*.[564] By contrast, a 2009 decision by the *Cour de Cassation*, France's supreme appeals court, held that *eBay* was a mere technical service provider. Its auction service fell therefore under the hosting liability privileges of the ECD. It only had to act if it acquired knowledge of manifestly illegal activity or information.[565] In another decision concerning the trademark rights of *L'Oréal,* the *Tribunal de Grande Instance of Paris* dissociated eBay's hosting activities and the making available of sales offers from its promotional activities that accompanied sales offers on the site. While the former were purely technical and indispensable activities for the function of an online marketplace, the latter were going beyond this and could therefore not qualify for the liability protections afforded to hosts.[566] This would in effect mean that the content liabilities would differ within the business activities of the same marketplace.

---

that is gathered from the behavioral data of clients of the multiple markets served by that company. Similarly, *eBay* has early expanded into classifieds and ticket sales, and for a time owned payment service *PayPal*.

563 *SA Louis Vuitton Malletier v eBay Inc and eBay International* [2008] 2010 ETMR 10 (Tribunal de Grande Instance de Paris, France) [188–189, 193].

564 *Hermès International v Feitz* [2009] Tribunal de Grande Instance de Troyes RG 06/02604. In : *L'Oreal SA v eBay International AG* (2009) E.T.M.R. 53 (High Court of Justice (Chancery Division)) [941].

565 *DWC v eBay France*, *eBay Europe* [2009] Cour de cassation, Chambre commerciale, Paris 08-11.672.

566 *L'Oréal SA c eBay France SA* [2009] Tribunal de Grande Instance de Paris RG 07/11365.

Belgian courts, on the other hand, have had less difficulty in qualifying e-commerce marketplaces as information hosts under the ECD. In *Lancôme v eBay* a Brussels court held that *eBay's* activities fell within the protections of Article 14 ECD.[567]

In Germany, courts were more concerned with the way in which the marketplace platform had 'appropriated' the content of the seller. In *Internetversteigerung I*, a case decided in 2004, the Federal Court of Justice (BGH) assessed that online marketplaces did not exercise any responsibility for the sales offers stored by them on behalf of third parties and that the hosting privileges of Article 14 took effect.[568] This line was continued in the *Internetversteigerung II* and *III* cases of 2007 and 2008.[569] The judgement also extended to (allegedly trademark infringing) advertisements, because these contents were not owned by the marketplace. German courts therefore appear to have looked strictly at whether content is stored on behalf of a third party and also took account of the fact that that storage occurred through the use of automated tools. The nature of the ancillary activities did not affect the classification as hosts under Article 14 ECD, as was done for example in the assessments of some French courts. However, these liability protection would not extend to injunctions.[570]

Marketplaces in the UK had a more difficult time to find refuge under the wings of the Article 14 protections for hosts. In one of the probably most high-profile cases, *L'Oréal* brought an action against e*Bay,* alleging, amongst others, that the latter could not avail itself of the hosting defence because its activities were going beyond mere technical and passive interventions. Again, it was claimed that *eBay* participated more actively in the sales process by organising and taking a part in the creation of information, namely advertising. Moreover, it promoted the sales offers and provided sponsored links to infringing products. Judge *Lord Arnold* voiced a preference for the arguments provided by claimant *L'Oréal* and agreed with the latter that *eBay* could have done more to prevent the sale of infringing goods via its site. However, he also noted the varying assessments and judgements concerning the liability of intermediaries across the EU.

---

567 *Lancôme v EBay, A/07/06032* (2008) (Unreported) (Tribunal de commerce de Bruxelles); *L'Oreal SA v. eBay International AG* (n 546) para 941.

568 *Internetversteigerung I (Rolex v Ricardo.de), Az I ZR 304/01* (2004) GRUR 2004, 860 (BGH) [863].

569 *Internetversteigerung II (Rolex v Ricardo.de)* [2007] BGH I ZR 35/04, JurPC-Web-Dok. 0108/2007; *Internetversteigerung III (Rolex v Ricardo.de), Az I ZR 73/05* [2008] MIR06/2008 (BGH).

570 *Internetversteigerung II (Rolex v Ricardo.de)* (n 568) para 19.

The interpretation of Article 14 ECD was far from clear and required clarification by the CJEU.[571]

ii. EU case law

The CJEU attempted to provide that clarification in one of its most influential rulings in the area of intermediary liability.[572] Apart from the question at hand, the CJEU's *L'Oréal v eBay* judgement also provided guidance on two other key ambiguities of the liability exemptions regime: actual knowledge and the preventive obligations of e-commerce marketplaces. In addition, the ruling gave clarification in the area of trademark law. An online marketplace operator, it said, did not make use of trademarks in the course of business where these trademarks were attached to goods sold by third parties via its website.[573]

L'Oréal had complained against repeated sales of perfumery products that infringed its trademark rights via the *eBay* marketplace. Of those products, some were counterfeits, but the majority were so-called grey imports and product samples, which were not destined for retail sales, but were nevertheless available via *eBay*. The French company also denounced the fact that *eBay* assisted the infringing sellers in the marketing of their products by selecting keywords in *Google's AdWords* program to display sponsored links on *Google's* search results pages to sales offers on its platform. These activities, it claimed, made *eBay* directly liable for violating *L'Oréal's* trademark rights. Failing that, *eBay* should at least be subject to an injunction aimed at preventing any future infringements of the trademarks in question.

The question about trademark liability and the availability of injunctions turned on the point of whether *eBay* could claim protection under the hosting provider defence of the ECD. The proceedings from the referring court demonstrated that the availability of the hosting defence for *eBay*'s activities was disputed and not clearly deductible from the text of

571 *L'Oreal SA v. eBay International AG* (n 563) paras 940–941. Further clarification was sought on whether sponsored links to infringing goods constituted trademark violations and the scope of relief available to trademark owners against intermediaries under IPRED 2004/48.

572 *L'Oréal v eBay* (n 463)

573 ibid 98–105.

the ECD.[574] The court therefore asked the CJEU whether *eBay's* activities were covered by the scope of Article 14 ECD. [575]

Like in *Google France*, the CJEU referred this question back to the referring national court for assessment based on the facts at hand. It provided, however, some indicative criteria to help national courts along in their assessments. The CJEU found that *eBay's* activities of setting the terms of service for sellers, storing the offer, providing general information to consumers and being remunerated did not impinge on the neutral role of an online marketplace. Assisting the seller by, e.g. optimising the display and promotion of offers, however, would point towards an active involvement of the marketplace and therefore the loss of the liability exemption.

iii. Application of CJEU rulings

Unfortunately, the referring UK court in *L'Oréal v eBay* never got the chance to apply the guidance provided by the CJEU. The case was settled out of court in 2014.[576] Notwithstanding the guidance provided by the CJEU, it remains disputed whether these rulings have brought the clarity sought. The judgement was very soon applied by various courts. However, despite the indicative criteria, national courts have assessed the role of e-commerce marketplaces in different ways, developing their own methodologies. Given the wealth of business models and functionalities, the constantly evolving nature of e-commerce, distinctive national legal traditions and different levels of awareness of technical detail, this is hardly surprising. National judges have therefore continued to this day to interpret the role of online marketplaces and the availability of the hosting defence in Article 14 ECD in different ways, which shall be illustrated in the following.

France

In 2012, a Paris appeals court, by referring to the CJEU's *L'Oréal v eBay* judgement, denied the marketplace the hosting provider status. It found

574 *L'Oréal SA v. eBay International AG* (n 563) paras 436–443.

575 *L'Oréal v eBay* (n 463) para 50 (9).

576 William Horobin And Greg Bensinger, 'L'Oréal, EBay Settle Dispute Over Counterfeit Goods' *Wall Street Journal* (15 January 2014) <https://www.wsj.com/articles/l8217or233al-eBay-settle-dispute-over-counterfeit-goods-1389816939> accessed 14 January 2020.

that through its "power seller" programme, *eBay* had actively promoted and assisted sellers in the sale of their products. These activities, the Paris court said, did go beyond mere storage of information. Indeed, *eBay* derived a direct profit from both the data stored and the goods sold. *EBay* hosted sales offers in order to support its principal activity of promoting products for its clients.[577] The French Supreme Court came to a similar result in 2012 when it confirmed decisions against *eBay* by lower instances in 2008 and 2010, brought by the *Luis Vuitton* owners *LVMH*. In this judgement, the French Supreme Court found that *eBay* provided the entirety of its sellers with information to help optimise their sales offers and the description and definition of their products. The marketplace was found guilty of selling counterfeit products and charged to pay EUR1.7 million to *LVMH*.[578]

By contrast, in 2012 the *Tribunal de grande instance de Paris* held in *Maceo*[579] that *eBay's* aforementioned promotional activities were solely aimed at improving and facilitating the searchability of offers. *EBay*'s technical design choices provided sellers with the opportunity to better structure, promote and market their products via its marketplace. That activity did, however, not mean that *eBay* selected and made decisions regarding the information that was put on its site. It did, therefore, not result in an active role of *eBay* in a sense that it had gained knowledge and control over information. Deriving an economic benefit from this activity did also not preclude *eBay's* classification as a hosting service. This outcome was confirmed in the same year in *Groupement des brocanteurs de Saleya v eBay's*. In an almost directly opposed reading of the CJEU judgement in *L'Oréal v eBay*, the *Cour d'appel de Paris* said that the optimisation of the presentation of offers, where it was automated and did not result in a modification of the content, could be considered as part of the technical service provided by the host.[580]

In the following years *Amazon*, *Alibaba* or *CDiscount* joined the ranks of *eBay* and appeared in front of French courts, again with varying results. The Chinese e-commerce behemoth *Alibaba* was denied the hosting

577 *eBay International v Burberry Ltd et autres* (2012) (Unreported) (Cour d'appel de Paris Pôle 5, Chambre 12).

578 *eBay Inc, eBay International v LVMH et autres* [2012] Cour de cassation (Surpeme Court) Chambre commerciale, financière et économique 11-10.508.

579 *Maceo v eBay International AG*, (2012) (Unreported) (Tribunal de grande instance de Paris, 3ème chambre, 1ère section).

580 *Groupement des brocanteurs de Saleya, CBA / eBay France et Ing* (2012) (Unreported) (Cour d'appel de Paris Pôle 5, chambre 1).

provider privilege in 2017.[581] The judges deemed that certain of its functionalities, e.g. a premium seller programme or structuring of the display of sellers and offers, visibly favouring Chinese sellers, corresponded to a specific commercial interest of the marketplace. *Alibaba* gave itself the appearance of a hosting service, while in reality it was an editor of information, playing an active role. It was found liable for offering counterfeit products and for unfair commercial practices. Meanwhile, French competitor *CDiscount*[582] was accorded the hosting provider status in a counterfeit action brought by apparel brand *Jansport* in 2019. The *Tribunal de Grande instance Paris* found that *CDiscount's* professional seller programme, the opportunity given to sellers to personalise and promote their offers, and to take part in a specific logistics program were either purely automated services, independent from the actual information stored, or did not lead to an active knowledge over the content. In a case concerning selective distribution agreements brought against *Amazon* and *Samsung,*[583] the former marketplace was also accorded the host status of Article 14 ECD. The *Cour de Cassation* mentioned *obiter dictum* that the claimant had failed to demonstrate that *Amazon* played an active role by offering: sellers to market their products internationally, i.e. on other *Amazon* country sites; payment services, notably cheque and bank card payments processing; product delivery, and to deal with problems arising during order fulfilment.

Germany

In 2011, a regional court in Stuttgart was one of the first to apply the CJEU ruling in Germany. It found that respondent *eBay* did not qualify for the host provider privilege because it had played an active role by promoting the offers of trademark infringing perfume products, owned by the applicant *Coty.*[584] This view was confirmed in the BGHs judgements in *Kinder-*

581 *Lafuma Mobilier v Alibaba et autres* (2017) (Unreported) (Tribunal de Grande instance, Paris).

582 *Jansport Apparel v Cdiscount* (2019) (Unreported) (Tribunal de Grande instance, Paris, 3ème chambre - 2ème section).

583 *Concurrence v Amazon services Europe, Samsung Electronics France* [2017] Cour de cassation - Chambre commerciale, financière et économique - 14-16.737, FR:CCASS:2017:CO01027.

584 *Coty Germany GmbH v eBay International AG (No1)*, [2011] LG Stuttgart, 17 Zivilkammer 17 O 169/11, [2012] ETMR 19 [46].

hochstühle II and *III*, of 2013 and 2015.[585] In this case *eBay* had selected keywords, relating to a brand of toddlers' high chairs in the *Google's AdWords* program. The search results from *Google* led to a list of offers that corresponded to a keyword search on *eBay's* platforms. This list included offers that infringed the trademark of the claimants, the owners of the brand of high chairs that corresponded to the keywords. In a direct application of *L'Oréal v eBay*, the BGH ruled that although the resulting product offer list was dynamic and automatic, *eBay* had an active role where it selected and booked *AdWords* campaigns on behalf of those sellers. It rejected *eBay's* argument that this service was purely automated and merely served as a neutral, supporting activity to the sale of goods undertaken by the sellers.[586] Meanwhile, the provision of automated tools aimed at creating and displaying product offers, sending promotional emails to customers and the option to manage sales transactions and payments did not lead to an active role of the marketplace.[587]

A regional court in Stuttgart applied the BGH's *Kinderhochstühle III* ruling in a case brought in 2018 against *Alibaba* by *Calvin Klein*. It added that offering different language versions of product detail pages and the existence of a buyer protection program by the platforms were also not sufficient for making *Alibaba* an active intermediary that had appropriated third party content.[588]

By contrast, marketplace *Amazon* was found liable for reproducing product images on its marketplace platform, because of the active role it played in selecting these images, which were uploaded by its sellers.[589] The claimant, who manufactures *Davidoff* perfumes, had a selective distribution agreement with *Amazon* and uploaded product images on that plat-

---

585 *Kinderhochstühle im Internet II, I ZR 216/11* [2013] MIR 2013 Dok 077 (BGH); *Kinderhochstühle im Internet III* [2015] BGH I ZR 240/12, 144/2015 JurPC WebDok.

586 *Kinderhochstühle im Internet III* (n 584) paras 85, 94–95. The same claimant had been less successful in 2012 in the Netherlands against the *eBay* subsidiary *Marktplaats (Stokke Nederland BV v Marktplaats BV* [2012] Gerechtshof Leeuwarden 107.001.948/01, NL:RBZLY:2007:BA4950. The Leeuwarden court ruled under virtually identical circumstances that, based on the CJEU criteria in *L'Oréal v eBay*, *Marktplaats* took a neutral position and was protected by Article 14 ECD.

587 *Kinderhochstühle im Internet III* (n 584) paras 81–82.

588 *Beeinträchtigung der Herkunftsfunktion einer Marke trotz Fälschungshinweises (Parfume Made in China)* [2018] LG Stuttgart, 17 Zivilkammer 17 O 928/13, GRURRS 2018, 20582 [53].

589 *Wiederholungsgefahr, 16 O 103/14* [2016] LG Berlin, 16 Zivilkammer DE:LGBE:2016:0126.16O103.14.0A, BeckRS 2016, 10918.

forms for the marketing of its products. A competing seller, who rightfully distributed similar products on *Amazon*, was allocated the same product images for its detail pages. The image selection was done through an algorithm deployed by *Amazon* and used for selecting the most suitable product images. The *Davidoff* licence holders complained. *Amazon* retracted the pictures but failed to make a cease-and-desist declaration. The marketplace argued that the selection of pictures was fully automated, giving its staff neither knowledge nor control over the decision over which images were allocated to an offer. The Berlin court found that it did not matter whether the selection process was done manually or algorithmically, as long as it was done by *Amazon* itself. By selecting the pictures *Amazon* "cut the decision chain between the seller and the picture." *Amazon* went therefore beyond being a purely neutral intermediary. Although this decision has been appealed, it remains remarkable as it somewhat counteracts a previous trend, at least in Germany, according to which marketplaces have not been found liable for erroneously or otherwise modifying product descriptions or price recommendations of sellers due to the fully automated nature of this activity.[590]

Finally, the ongoing challenges on assessing the role of today's intermediaries can be seen from the recent CJEU ruling in *Coty v Amazon*.[591] In this case the perfume manufacturer claimed that *Amazon's* activities as a marketplace operator in conjunction with its logistics service for sellers, *Fulfillment by Amazon (FBA)*, went beyond a merely neutral role. The vertically integrated activities, through which grey market goods sold by third party sellers were offered and shipped to customers, led to *Amazon* making use of *Coty's* marks in the course of business, thus constituting violations of its trademark. This view was not shared by the CJEU, which also partly contradicted the assessment offered by the AG.[592] The CJEU looked at *Amazon's* marketplace operations and its fulfilment service individually. Each of these services taken in isolation were intermediary activities for

590 Bernhard Knies, 'Amazon Haftet Für Urheberrechtsverletzungen Seiner Verkäufer' (*new-media-law.net*, 9 June 2016) <https://www.new-media-law.net/amazon-haftet-fuer-urheberrechtsverletzungen-seiner-verkaeufer/> accessed 17 January 2020; *Haftung für falsche UVP-Angabe bei Amazon* [2015] OLG Köln 6 W 29/15, openJur 2016, 3226.

591 *Coty Germany GmbH v Amazon Services Europe Sàrl and others, C-567/18* [2020] EU:C:2020:267 (CJEU).

592 *Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona, Coty Germany GmbH gegen Amazon Services Europe Sàrl und andere, C-567/18* [2019] EU:C:2019:1031 (CJEU).

which case law had confirmed that they did not make use of trademarks in the course of business. It implied that marketplace operations would need to be examined under Article 14 ECD, while the storage activities fell under Article 11 IPRED.[593] This case serves as a fitting example over the difficulties of assessing the status of online intermediaries in the dynamically evolving platform economy.[594] It also demonstrates the challenges of the current ECD framework, which looks at liability and the regulation of intermediaries by applying a rather narrow neutral/passive dichotomy. This appears to be oddly out of place with current realities. Online platforms have for some time started to expand into and transform more traditional "physical" activities of the wider economy and integrated them into other business models. This makes the distinction between electronic and non-electronic services which the ECD relies on in its functional scope for regulating ISSPs all the more challenging. This judgement will be analysed in more detail in the trademarks section of Chapter 4.

UK

UK courts applied the CJEU ruling of *L'Oréal v eBay* in *Cosmetic Warriors v Amazon*.[595] *Cosmetic Warriors* is the owner of the *Lush* cosmetics brand and brought *Amazon* to court for trademark infringements. Using an autocomplete functionality, *Amazon* customers' searches were completed with *Lush* product names and suggestions, resulting in the display of competing sales offers, which did not bear the *Lush* trademark. These products were either sold by Amazon itself or by third party sellers on its marketplace, some of them also utilising the *Amazon FBA* logistics service. Applying *L'Oréal v eBay*, the English court had relatively little difficulty in finding Amazon's activity "much more than merely use in a service consisting of enabling its customers to display on its website signs corresponding to trade marks."[596] Although the display of products sold and shipped by third party sellers may not be infringing use, the list of search results was mixed with those products that were sold by *Amazon* itself and those sold by third-part sellers using the e-commerce giant's fulfilment service *FBA*. For the latter two categories *Amazon* clearly engaged in commercial communication to pro-

593 *Coty v Amazon (FBA)* (n 590) para 49.
594 Carsten 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' (2019) 14 Journal of Intellectual Property Law & Practice 5.
595 *Cosmetic Warriors v Amazon* (n 560).
596 ibid 57.

mote its own activities. This reading is remarkable because it somewhat pre-confirms the opinion of the CJEU's AG Campos Sánchez-Bordona in *Coty v Amazon.* The AG had indicated that the fulfilment and marketplace activities of Amazon, seen jointly, could be seen as active involvement and trademark use.[597]

The rulings above show that courts in Europe have to this day had marked difficulties in evaluating the role of marketplaces in the intermediation process. The technical architecture, supporting services (promotional activities, sales optimisation, payment and logistics services) and the changes in business models have caused veritable headaches to judges. E-commerce marketplaces are therefore a fitting example of the changing nature of online intermediaries. Over the last 10 years at least, e-commerce marketplaces have engaged in online marketing activities (on site, advertising on third party sites), have built sophisticated search engine functionalities, integrated other intermediary service providers (payment, third party logistics), offered their ancillary services (buyer insurance, logistics services), and diversified their product choice (integrating own products, international/global selling). As a result, courts have continued to struggle when pinning down the role of e-commerce marketplace in the intermediation process and the availability of the ECD's hosting defence, even in the wake of the supposedly clarifying rulings by the CJEU.

iv. US developments

US courts, by contrast, have been more consistent in according the liability protections to these internet intermediaries. In the earlier cases of *Stoner,*[598] *Hendrickson*[599] and *Tiffany*[600] the courts confirmed that intermediary *eBay*, who was the defendant in all three cases, qualified for the protections offered to internet intermediaries under the CDA, the DMCA and the Lanham Act, respectively. Thus, in *Hendrickson*, a case involving the sale of pirated video DVDs, the judges had no doubt that *eBay* qualified for the safe

597 *AG Opinion, Coty v Amazon (FBA)* (n 591) paras 59–62.
598 *Randall Stoner v EBay Inc, et al* [2000] Sup Ct Ca Civ. No. 305666, (Unreported).
599 *Hendrickson v eBay* [2001] CD Cal CV 01-0495 RJK (RNBx) (C.D. Cal. 2001), 165 F. Supp. 2d 1082.
600 *Tiffany (NJ) Inc v eBay Inc* (2010) 600 F. 3d 93 93 (2nd Cir).

harbour provisions offered by the DMCA.[601] Similarly in *Tiffany*, the jewellery maker complained against the massive sale of counterfeits on *eBay*, which infringed its trademark. Here, the availability of protections against secondary infringements by intermediaries under the Lanham Act were confirmed.[602] More recently, the very narrow interpretation of (secondary) liability was confirmed for the new type of e-commerce marketplaces.[603] In *Milo Gabby v Amazon*,[604] a pillow manufacturer brought *Amazon* to court over the repeated sale of "knock-off" versions of its products. The company argued that at least for those sellers using the *FBA* service the marketplace acted as a seller with enhanced liability for the products on offer. The Court found, however, that *Amazon* did not take ownership of the goods through its FBA service, and that "even if Amazon were to take title under the Fulfillment by Amazon agreement, it would do so only to dispose of the product, not to sell it."[605] This is in marked contrast to the view of the platform's involvement by the CJEU's AG in *Coty v Amazon*, but also the UK judgement in *Cosmetic Warriors v Amazon*.

c. UGC platforms and social networks

Social media and UGC platforms' new interactive and immersive qualities when it comes to the dissemination of information have already been introduced in Chapter 2. Similar to e-commerce marketplaces, courts have grappled with problems in according these intermediaries the immunity status as hosting providers under Article 14 ECD. The variety of potentially unlawful content spread via these sites is much larger than compared to e-commerce marketplaces. UGC and social media sites have been in the focus for their involvement in the spread of copyright infringing content,

601 According to the US' DMCA 17 U.S.C. § 512 (c) (1), intermediaries will merely not have to have actual knowledge of unlawful activity, do not directly benefit financially from it and remove such content expeditiously once notified of it.

602 Andrew Lehrer, 'Tiffany V. EBay: Its Impact And Implications On The Doctrines Of Secondary Trademark And Copyright Infringement' (2012) 18 Boston University Journal of Science & Technology Law 32, 389–400.

603 R Bruce Rich and David Ho, 'Sound Policy and Practice in Applying Doctrines of Secondary Liability Under U.S. Copyright and Trademark Law to Online Trading Platforms: A Case Study' (2020) 32 Intellectual Property & Technology Law Journal 15, 9–10.

604 *Milo & Gabby LLC v Amazon.com* [2017] Fed Cir 2016-1290, 693 F. App'x 879.

605 ibid.

hate and terrorist speech, defamatory content, and child abuse material as well as counterfeits or illegal products.

i. National case law

France

In France, the early social networking site *MySpace's* was seen as a publisher of content, thus forfeiting the hosting provider liability protection under the ECD.[606] In this 2007 case, the *Tribunal de Grande instance de Paris* found that *MySpace* had structured the design of user accounts pages and displayed dynamic adverts from which it generated revenue. These activities inferred control and knowledge of the information stored.[607] Consequently, *MySpace* was found directly liable for copyright infringement and obliged to prevent uploads of illegal (copyright infringing) content. It is interesting to note that under similar circumstances *Dailymotion*, a French video sharing platform (VSP) was found to be a host provider in 2010. In that case the judges argued that making available a pre-structured design and providing tools for classifying content was a pure technical necessity for the act of hosting under *Dailymotion's* business model.[608] Already in 2007, when a film producer sued the platform for copyright infringements and parasitic conduct, had this VSP been accorded the status of a host provider.[609] Nevertheless, the French judges still refused to accord *Dailymotion* the liability protections. Because its (hosting) business model relied on the infringing activity by its users, it was inevitable that it had actual knowledge of these unlawful acts.[610] This approach was confirmed in a case against *Google Video* in 2008.[611]

---

606 *Jean Yves L dit Lafesse v Myspace* (2007) (Unreported) (Tribunal de grande instance de Paris).

607 ibid., see also : Angelopoulos, 2009, p. 3

608 *Roland Magdane et autres v Dailymotion* (2010) (Unreported) (Cour d'appel de Paris Pôle 5, chambre 1). Under the judgement's heading: *Sur la nature du service offert par la société Daily Motion*

609 *Christian, C., Nord Ouest Production v Dailymotion, UGC Images* (n 196). Under Chapter « DISCUSSION Sur la nature de l'activité exercée par la société Dailymotion et sa responsabilité ».

610 See also the discussion in: Christina Angelopoulos, 'Filtering the Internet for Copyrighted Content in Europe' (2009) 4 iris plus 12.

611 *Flach Film et autres v Google France, Google Inc* (2008) (Unreported) (Tribunal de commerce de Paris 8ème chambre).

The tendency of granting UGC sites the status of hosts under the ECD was somehow disrupted by the French Supreme Court's 2010 ruling in *Tiscali Media*.[612] Despite agreeing that *Tiscali* was not a publisher of the personal pages that they assisted users in creating, the company engaged in more than mere technical activities required of a hosting provider. For example, *Tiscali* offered to place advertisements on the personal pages of their users, including on pages containing copyright infringing content. By benefitting from this activity, *Tiscali* became more than a simple technical host of information and took over a responsibility for the unlawful content.[613]

Germany

By contrast, German courts were less hesitant initially in qualifying UGC services as host provider. The test to determine the active /neutral role corresponded to an evaluation of whether the platform had appropriated ("*sich zu Eigen Machen*") the content hosted on behalf of a third party.[614] This line was established by the BGH in *Marion's Kochbuch*.[615] *Marion's Kochbuch* was an internet portal that made cooking recipes uploaded by users publicly available. The portal was found taking possession of the content by verifying it for completeness and accuracy before sharing it amongst its users. In addition, the portal providers had obtained rights to monetarise the content, including marketing it to third parties. In the following *Rapidshare* and *GEMA v YouTube* cases,[616] the application of hosting provider privileges caused markedly less headaches to the German courts. In an ongoing saga of several cases for a period of over 10 years, *GEMA*, the German music authors and publishers' rights association, claimed that *YouTube* engaged in infringing acts by making works publicly available without having received the authorisation for it. The Hamburg court distinguished this case from *Marion's Kochbuch*. Notably, *YouTube* did not need to check uploaded content for its correctness before sharing

612 *Télécom Italia (Tiscali) v Dargaud Lombard, Lucky Comics* (2010) (Unreported) (Cour de cassation 1ère chambre civile).

613 See also: Tobias Bednarz, 'Keyword Advertising before the French Supreme Court and beyond - Calm at Last after Turbulent Times for Google and Its Advertising Clients?' (2011) 42 International Review of Intellectual Property and Competition Law 641, 653–655.

614 Nolte and Wimmers (n 551) 20–21.

615 *Marion's Kochbuch* [2009] BGH I ZR 166/07, MIR 2010, Dok. 082.

616 *RapidShare II* [2012] OLG Hamburg 5 U 87/09, MMR 2012, 393; *GEMA v YouTube* (n 264).

it. Activities such as structuring or categorisation of content did not result in *YouTube* having editorial or active control.[617] Likewise, the fact that *YouTube* exploited third-party content economically, through sub-licencing and advertising, was insignificant. Users were offered the possibility to withdraw the permission for this activity at any time.[618]

Italy

In Italy, courts went yet a slightly different way in determining the availability of the hosting defence for UGC platforms, notably *YouTube*. Faced with the complexities of the activities of these platforms they developed the concept of "active hosting providers." This may also reflect an attempt to fit the new activities of Web 2.0 platforms to the categories of intermediary liability available through Italian national law.[619] Thus, in 2011, the VSPs *IOL* and *Yahoo!* were classified this way. The determining factors were that they carried advertising on detail pages that contained infringing content; that they reserved themselves the right to edit or modify uploaded content; and that they provided an internal search engine functionality. Moreover, they were themselves engaged in uploading content. In the end they were seen as hosts, albeit with an active role, and therefore directly at fault for copyright infringements.[620] The latter judgement was overturned in 2015 when the appeals court disapproved of the active hosting provider category and ruled that the service in question was neutral.[621] Finally, in 2019, the Italian Supreme Court qualified the previous rulings by affirming the active hosting provider doctrine of the Italian judiciary. It pointed out a number of activities that can be seen as indicative for active behaviour of the hosting service, such as indexing, selecting, filtering, organising, promoting or aggregating content. An active host would lose the protections of Article 14 ECD. However, the previous appeals court had correctly ruled that *Yahoo* was passive.[622]

---

617 *GEMA v YouTube* (n 264) para B V 2 a bb.

618 ibid B V 2 b.

619 See Ch 3. B. 2. II. b

620 *Reti Televisive Italiane S.pA v Italia On Line S.r.l* [2011] Court of Milan 3821/11; *Reti Televisive Italiane S.pA v Yahoo! Italia S.r.l and Yahoo! Inc*, (2011) (Unreported) (Court of Milan). In: E Bonadio and M Santo, 'Court of Milan Holds Video Sharing Platforms Liable for Copyright Infringement' (2012) 7 Journal of Intellectual Property Law & Practice 14.

621 Giulio Coraggio, 'Internet Litigation.' (2015) 21 IP Litigator 25.

622 *Reti Televisive Italiane SpA v Yahoo! Inc and Reti Televisive Italiane SpA v Yahoo! Inc* [2019] Court of Appeal of Milan 7708/19 and 7709/19. In: Eleonora Rosati,

In the same vein, VSP *YouTube* was qualified as a passive host in 2017, with its indexing and content organisation activities being seen as not altering the content itself.[623] Its competitors *Dailymotion* and *Vimeo* were, meanwhile, seen as active hosts two years later, and not in a position to make use of the liability protections of the ECD. In the latter case, the fact that *Vimeo* had set up its own search engine, categorised and indexed content uploaded by users, and linked the display of advertisings to user searches all confirmed its active character.[624] *Facebook* also forfeited the hosting privilege entirely as a result of being held directly responsible for copyright infringing acts.[625]

UK

In the UK defamation case of *CG v Facebook*, a Northern Irish appeals court accorded the social network the immunities of Article 14 implicitly and without any further test of its activities.[626] In contrast to cases involving e-commerce marketplaces, this appears to be a common line in UK jurisprudence on social media platforms.[627] At least, however, the hosting provider status of UGC sites and social media platforms is not challenged

---

'Italian Supreme Court Clarifies Availability of Safe Harbours, Content of Notice-and-Takedown Requests, and Stay-down Obligations - The IPKat | Diigo' (*The IPKat*, 20 March 2019) <https://ipkitten.blogspot.com/2019/03/italian-supreme-court-clarifies.html> accessed 23 January 2020.

623 *Delta TV v Google and YouTube* [2017] Turin Court of First Instance (Tribunale di Torino) No. 1928, RG 38113/2013. In: Eleonora Rosati, 'Italian Court Finds Google and YouTube Liable for Failing to Remove Unlicensed Content (but Confirms Eligibility for Safe Harbour Protection)' (*The IPKat*, 30 April 2017)

624 *Mediaset v Dailymotion* [2019] Rome Court of First Instance 14757/2019; In: ibid. *Reti Televisive Italiane S.p.a (RTI) v Vimeo* [2019] Tribunale di Roma 623; in: Ernesto Apa and Bassini, 'Court of Rome Rules Vimeo Liable for Copyright Infringement' [2019] iris Newlsetter 50.

625 *Mediaset v Facebook* [2019] Rome Court of First Instance 3512/2019. In: Eleonora Rosati, 'Facebook Found Liable for Hosting Links to Unlicensed Content' (*The IPKat*, 21 February 2019) <http://ipkitten.blogspot.com/2019/02/facebook-found-liable-for-hosting-links.html> accessed 23 January 2020.

626 *CG v Facebook Ireland Ltd & Anor* [2016] 2016 NICA 54 (Court of Appeal in Northern Ireland) [53]. See also for more detailed discussion: Lorna Woods, 'When Is Facebook Liable for Illegal Content under the E-Commerce Directive? CG v. Facebook in the Northern Ireland Courts' (*Inforrm's Blog*, 28 January 2017) <https://inforrm.org/2017/01/28/when-is-facebook-liable-for-illegal-content-under-the-e-commerce-directive-cg-v-facebook-in-the-northern-ireland-courts-lorna-woods/> accessed 23 January 2020

627 *J20 v Facebook Ireland Ltd* [2012] High Court Of Justice In Northern Ireland Queen's Bench Division COL10121 [48].

by the courts. In *Galloway v Frazer* the Northern Irish court declined to settle this particular matter without being specifically asked, and examined *Google's* conduct practically under the premise that it was a hosting provider.[628]

ii. EU case law

The first, and so far, only attempt by the CJEU at a clarification on the availability of the hosting defence for social networks site came from the *Netlog* case in 2012.[629] *Netlog* was a Belgian social media network, which was brought to court by the Belgian association of music authors and rightsholder (*SABAM*). *SABAM* tried to impose an injunction forcing *Netlog* to stop the unauthorised sharing of music for which it owned the copyright. The CJEU found no difficulty in according the hosting provider status to the social network, noting that "it is not in dispute that the owner of an online social networking platform - such as Netlog - stores information provided by the users of that platform, relating to their profile, on its servers."[630] One had to wait until the recent *Facebook*[631] ruling to see the CJEU pronounce itself on the availability of the hosting defence for a social networking platform. In that judgement the CJEU, however, just said that it was common ground that *Facebook* provided a service that qualified for protection under the hosting provider regime of the ECD. A small glimpse of doubt is, however, gleaned from AG Szpunar's Opinion on this case. He remarks curiously and seemingly in passing that the assessment of the referring court accorded *Facebook* the status of a hosting provider *"irrespective of the doubts that one might have in that regard."*[632]

It seems the *CJEU* did not want to trouble itself with this potentially thorny issue. Another explanation may be that, since in *Google France* and *L'Oréal v eBay* the CJEU had referred the detailed assessment on the neutral/passive role on the platform back to national courts, it did not want to pronounce itself further without being specifically asked.

628 *Galloway v Frazer, Google Inc (YouTube) and Ors* [2016] Northern Ireland Queen's Bench Division HOR979, [2016] NIQB 7 [7].
629 *SABAM v Netlog* (n 460).
630 ibid 27.
631 *Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 463).
632 *Opinion of Advocate General Szpunar on Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 264) para 30.

That chance will however present itself in the future. There are currently two referrals by the Austrian and German Supreme Courts in front of the CJEU which aim to establish clarity on the availability of the hosting defence for the VSP *YouTube*.[633] The plaintiffs seek guidance on whether various activities of *YouTube* conferred on it an active role, outside of the hosting provider status of the ECD. These activities consist, amongst others of: providing users with the possibility to search, flag and comment on videos, making advertising and licencing revenue from the shared content, structuring content, such as by sorting and ranking, as well as recommending clips to users. It appears logic that any decision taken for the UGC site *YouTube* would have repercussions on the activities of social networks like *Facebook*, through which also various types of content are being shared, recommended and advertised on a similarly massive scale.

This hands-off approach by the CJEU was confirmed in the *SNB-REACT* ruling. The Estonian Court of Appeal in Tallinn had asked the CJEU whether internet registries and registrars could qualify for the ECD's liability protections.[634] The case was brought by *REACT*, an industry association that defends trademark owners' rights, against a provider which offered services for rental and registration of IP addresses. This service had registered 38,000 IP addresses and domain names which were in violation of *REACT* members' trademark rights. The CJEU stated, however, that first it was for the referring court to determine whether IP address rental and registration services fulfilled the criteria of an ISSP. Secondly, that court would also need to assess that the service met the detailed criteria of Articles 12 – 14 ECD, including the decision which kind of intermediary these services would be. The court cited almost *ad verbatim* its iterations in *Google France* and *L'Oréal v eBay*.

633 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) (CJEU); Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 1 July 2019 — Puls 4 TV GmbH & Co KG v YouTube LLC and Google Austria GmbH (Case C-500/19) (CJEU).

634 *Coöperatieve Vereniging SNB-REACT U.A. v Deepak Mehta - C-521/17* (n 276) paras 47–52.

II. The intermediary's actual knowledge of illegal acts

a. Defining actual knowledge

Online intermediary service providers that act merely technical and passive will qualify for the liability exemptions offered by Articles 12 – 14 ECD. Caching and hosting services will not be liable for any illegal information or activity that they had no actual knowledge of.[635] Once they obtain that knowledge they need to remove the information expeditiously or block access to it. An additional condition applies to hosting providers. They must not be aware of facts and circumstances from which illegal information or activity is apparent.[636] Mere conduits, by contrast, only need to respond to court or administrative orders to terminate or prevent infringements.[637]

As mentioned above, throughout common and civil law systems knowledge has been used as a condition to determine fault and subsequent liability of intermediaries. Not all Member States did, however, transpose the actual knowledge requirement of the ECD literally into their national laws. The Netherlands merely refer to liability only where an intermediary knew of unlawful acts or activity or could have been reasonable expected to know. The Czech Republic and Spain tie actual knowledge directly to the receipt of a notice. Germany and Portugal just refer to knowledge, instead of actual knowledge.[638]

But even where Member States did follow a word-by-word transposition of the ECD, courts still risked at coming to different interpretations of actual knowledge. As concluded by Judge Arnold in the *Newzbin* case "the interpretation of the requirement of 'actual knowledge'… is primarily a matter of domestic law, albeit within the framework created, and the constraints imposed, by European law."[639]

Courts faced notable problems when trying to establish the circumstances under which an intermediary could be presumed to have attained actual knowledge that would trigger an obligation to act. This question is linked first to the definition of actual knowledge. In the UK case of *Newzbin*, for example, it was found that actual knowledge was related to

635 Directive 2000/31 (ECD) Article 14 para 1 (a) (b), Article 13 para 1..
636 Ibid. Article 14 para 1 (a).
637 *Mc Fadden* (n 139) paras 63–65.
638 Verbiest and others (n 315) 34–35. European Commission, 'SEC(2011) 1641 Final' (n 11) 32–37.
639 *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] 2011 EWHC 1981 Ch (High Court of Justice Chancery Division) [202].

the extent to which a service provider knew about particular persons being involved in particular restricted acts, involving particular copyrighted works.[640] This reasoning implies that actual knowledge is linked to subjective knowledge of the service provider of infringing activity. This reading is confirmed by German case law, where actual knowledge has been interpreted as knowledge of specific unlawful acts or content by a human being. By contrast, general awareness of illegal activity cannot be equated to actual knowledge.[641]

The requirement of awareness of facts and circumstances indicating illegal activity, which may result in pecuniary damages, if not addressed,[642] is likened to the tort of gross negligence. This can also be "objective knowledge", or facts, which a person or actor in comparable circumstances should or could have been expected to be aware of. Another early consensus that arose from national court rulings was that intermediaries were supposed to attain actual knowledge or actionable awareness where it concerned manifestly illegal information or activity. However, the definition of manifestly illegal content varies by country. While there is little difference nationally over the manifestly illegal nature of child pornographic content, it appears that courts have applied different knowledge standards when it came to less obvious areas such IP law or defamation.[643]

b. Obtaining actual knowledge

Following jurisprudence at national and EU level there are usually three ways of how an intermediary service provider may obtain actual knowledge. First, through notification by an authority or court. Secondly, the notice can be given by an allegedly damaged party, such as an IP rightsholder or a defamed person. The third method has been much more controversially discussed. It relates to an intermediary being aware of facts or circumstances that indicate illegal activity and thus being obliged to act under the ECD.[644]

640 ibid 148.
641 Verbiest and others (n 315) 37.
642 Directive 2000/31 (ECD) Article 14 (1) (a).
643 Verbiest and others (n 315) 36–41.
644 European Commission, 'SEC(2011) 1641 Final' (n 11) 33.

i. Court or authority orders

Orders from a court or an authority may be the most obvious way for an intermediary to gain such actual knowledge. This is because the intermediary would not need to engage in his own assessment of whether the notified content is indeed illegal under the laws of the respective jurisdiction. Spain, for example, defined in its national transposition of the ECD the term actual knowledge explicitly as only relating to such instances where a competent authority has declared such content illegal and notified the intermediary.[645] While this may be the safest way to avoid mistakes and erroneous or over-cautious blocking of legal content, it is questionable that this would be an effective way of dealing with the vast amounts of illegal content. In addition, it may relieve intermediaries of any duty at all and therefore render the knowledge requirement superfluous.[646]

ii. Notice-and-Takedown

Notification by private third parties can be seen as the standard procedure under the current ECD regime, and under intermediary liability regimes worldwide, of providing intermediary service providers with actual knowledge of illegal content or activity. This procedure is globally known as notice-and-takedown (NTD) or notice-and-action (NA). Upon receipt of a notice, it is the responsibility of the intermediary to decide on the claim's veracity. The safe harbour protection would apply if the online intermediary removes or disables access to the notified unlawful content or activity.[647] The US intermediary provisions of the DMCA operate on the same principle for hosting services and for search engines.[648]

Unlike US law, the ECD does not lay down requirements for the process and format of NTD requests. This means that the details required to put an intermediary on actionable notice vary across Member States. The latter may or my not regulate these details through their national laws for hosting providers established in their jurisdiction.[649] The EU has set out in the

645 Thibault Verbiest and others, 'Study on the Liability of Internet Intermediaries, Markt 2006/09/E - Country Report Spain - Executive Summary' 2; Rowland, Kohl and Charlesworth (n 128) 86.
646 Rowland, Kohl and Charlesworth (n 128) 86.
647 Directive 2000/31 (ECD) Article 13 (1) (e), 14 (1) (b).
648 17 U.S.C. § 512 c (1) (A) (iii), d (1) (c).
649 Directive 2000/31 (ECD) Article 14 (3).

ECD that measures to formalise NTD should rely on self-regulation, such as codes of conducts.[650]

Some Member States have decided to implement such requirements through national or soft law provisions. Most of the time, these processes did not follow the broad horizontal remit of the ECD, but were put in place for specific content sectors, such as copyright, or child abuse content, or for only certain types of intermediaries. According to a 2012 European Commission study, nine Member States had implemented NTD procedures in their national laws.[651] Sweden and Portugal had put in place horizontal NTD frameworks for hosting providers that covered any type of infringement. However, only in Portugal does compliance with the procedures set out in the NTD framework protect intermediaries explicitly from liabilities. Finland, France, Hungary, Lithuania, the UK and Spain have put NTD procedures in place for copyright violations. Germany put in place notification procedures for child pornographic material and the UK for terrorist content. The requirements on the format and content of notices under these national regimes, for example, whether it should contain an URL, a description of the violation, a proof of authority, varied widely, as did the time limits set for reacting to a notice or for filing counterclaims. More recently, Germany and France have introduced or proposed laws aimed at codifying notification and removal procedures for hate speech on social media and UGC platforms.[652]

In addition, in many Member States, industry led, self - regulatory procedures have been set up, which are aimed at formalising NTD in specific sectors. In Austria, Belgium, Denmark, France, Germany, the Netherlands and the UK, industry and trade associations have set up code of conducts for their members concerning the reporting and removing of unlawful content.[653] Some of the more well-known industry led projects in the area of notifying and removing child abuse content on the internet are the

650 ibid Recital 40, Article 16 (1).

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

652 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken 2017 (BGBl I S 3352 (Nr 61)); Laetitia Avia, Proposition de loi visant à lutter contre la haine sur internet.

653 Verbiest and others (n 315) 110–115. Swiss Institute of Comparative Law, 'Study on Filtering, Blocking and Take-down of Illegal Content on the Internet' (Council of Europe 2015) 796–800 <https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet> accessed 4 February 2020.

UK's *Internet Watch Foundation* and Germany's *Association for Voluntary Self-Regulation of Digital Media Service Providers (FSM)*.[654]

In the absence of any guiding procedures in national law on NTD, courts have also stepped in and decided on a case by case basis whether notices where sufficient to confer actual knowledge of the existence of illegal content. For example, in 2007, a Belgian judge specified the details of a copyright infringement notice and the time limit for reaction in a case involving the intermediary *Google News*.[655] Until as recent as 2019, Italian and French courts have given guidance on the level of detail required for notices in copyright and trademark infringement that would give intermediaries actual knowledge.[656]

Meanwhile, larger, global, often US-based online platforms that determine the intermediary landscape of today have put in place their own notification systems on their platforms.[657] These are largely based on the more detailed US legal requirements, as for example set out by the DMCA. They are adapted, where necessary, to local requirements. In the absence of any fixed rules, these systems have become the quasi standard for NTD.

The meaning of "expeditious" removal of unlawful information is less of a contested issue. With the incredible surge in NTD requests that many of the larger platforms receive today, especially in the area of copyright, these activities are by now largely automated and operationalised. Where the public interest is at a higher stake, such as for terrorist content, the EU and Member States have started to formulate more onerous review and removal timelines.

---

654 'Our Members' (*IWF*) <https://www.iwf.org.uk/become-a-member/join-us/our-members> accessed 4 February 2020; 'FSM | About Us' <https://www.fsm.de/en/about-us> accessed 4 February 2020.

655 *Copiepresse et al v. Google Inc* (n 555).

656 For Italy: Eleonora Rosati, 'Italian Supreme Court Clarifies Availability of Safe Harbours, Content of Notice-and-Takedown Requests, and Stay-down Obligations - The IPKat | Diigo' (*The IPKat*, 20 March 2019) <https://ipkitten.blogspot.com/2019/03/italian-supreme-court-clarifies.html> accessed 23 January 2020; for France: *Jansport Apparel v Cdiscount* (Tribunal de Grande instance, Paris, 3ème chambre - 2ème section).

657 'How to Report Things on Facebook | Facebook Help Center' <https://www.facebook.com/help/181495968648557/> accessed 4 February 2020; 'Amazon.de - Mitteilung an Amazon.de Über Eine Rechtsverletzung' <https://www.amazon.de/report/infringement?> accessed 4 February 2020; 'Copyright Infringement Notification - YouTube' <https://www.youtube.com/copyright_complaint_form> accessed 4 February 2020; 'Signaler les comportements inappropriés' <https://help.twitter.com/fr/safety-and-security/report-abusive-behavior> accessed 5 February 2020.

CJEU guidance on this matter has not been overly helpful. In *L'Oréal v eBay*, the EU's highest court simply stated that for a notification to eventually lead to awareness of illegal information or activity, it must be sufficiently precise and adequately substantiated. Whether that was the case in a given situation was a matter for national courts to decide upon.[658]

The resulting patchwork of notification and removal standards across the EU has been recognised as a barrier to the effective and transparent removal of unlawful information on online platforms, including by the European Commission.[659] For one, the current situation still leads to varying interpretations of the level of detail needed in a notification that leads to actual knowledge. Secondly it obliges intermediaries operating across Member States to comply with various notification standards, which runs counter to the original aim of the ECD to establish clear and general rules that regulate the activities of ISSPs.[660] Thirdly, it hinders the establishment of EU wide, consistent and transparent notification procedures that are not only effective, but also safeguard fundamental rights, such as freedom of expression, privacy, the right to exercise a business and intellectual property. This is important because of intermediaries' role as "private judges" over the legality of content, especially in cases where content is not manifestly or obviously unlawful. Notorious areas in this respect are exemptions provided in copyright or borderline speech that may be differently regulated by national laws.[661]

The latter problem is accentuated by the emergence of mass notifications in certain areas, such as IP rights. Major platform operators, such as *YouTube*, or *eBay* have been responding to this with automated takedown systems which have been found to lead to over-blocking and chilling effects on freedom of expression, while at the same time not adequately protecting IP rights.[662] These problems are even more apparent with regards to voluntary measures taken by platforms to prevent illegal information,

658 *L'Oréal v eBay* (n 463) paras 121–122.

659 European Commission, 'C(2018) 1177 Final' (n 8) Recitals 11, 12.

660 Directive 2000/31 (ECD) RECITAL 7.

661 European Commission, 'SEC(2011) 1641 Final' (n 11) 45–46. Sebastian Felix Schwemer, 'Trusted Notifiers and the Privatization of Online Enforcement' (2019) 35 Computer Law & Security Review 105339.

662 Lilian Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' in Lilian Edwards (ed), *Law, policy, and the Internet* (Hart 2019) 272–277. Jennifer M Urban, Joe Karaganis and Brianna L Schofield, *Notice and Takedown in Everyday Practice* (American Assembly 2016).

which will be discussed below and in the relevant content subject matter sections of Chapter 4.

The European Commission did not identify any immediate need for the establishment of EU wide NTD procedures in the ECD evaluation exercises of 2003 and 2007. Following feedback received from a 2010 public consultation, which substantiated the problems outlined above,[663] the European Commission committed, as part of its Digital Agenda for Europe, to "adopt a horizontal initiative on notice and action procedures" subject to an impact assessment.[664] From 2016 to 2018 the Commission then committed to reviewing the need for formal notice and action procedures, however, with a view to do this on a sectoral level.[665] These intentions were accompanied by a number of EU Codes of Conduct and Memoranda of Understanding[666] aimed at establishing sectoral standards for the identification and removal of unlawful content. These will be discussed in the next chapter.

Finally, in its 2018 Recommendation, the Commission provided a number of general minimum procedural recommendation on NTD in order to safeguard fundamental rights. This covers information requirements to content providers and counter notice procedures, but does not go into further detail on the information that a notice should contain. The proposed Digital Services Act (DSA) now proposes for the first time legally binding procedural requirements for NTD for hosting services, and enhanced procedural obligations for the new category of online platforms.[667]

It is important to state that throughout the EU and its Member States, policy makers see NTD as a central element by which online intermediaries will receive actionable knowledge of unlawful information and activity. This is despite the growing importance attached to voluntary, proactive investigations on the part of online platforms. However, the nature of NTD has also been enriched by collaborative technology. User engage-

663 European Commission, 'SEC(2011) 1641 Final' (n 11) 39–46.

664 European Commission, 'A Coherent Framework for Building Trust in the Digital Single Market for E-Commerce and Online Services, COM(2011) 942 Final' (European Commission 2012) 14–15.

665 European Commission, 'COM(2016) 288 Final' (n 223) 8–9; European Commission, 'COM(2017) 228 Final' (n 538) 9.

666 'Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet, 2011' <https://perma.cc/DF6M-JNJ8> accessed 29 June 2020; 'Memorandum of Understanding on the Online Sale of Counterfeit Goods, 2016' (n 542); 'Code of Conduct on Countering Illegal Hate Speech Online' (n 542).

667 European Commission DSA proposal (n 10) Articles 14, 17 and 19.

ment, for example through trusted flaggers or trusted notifier systems has received increasing policy attention, although there are reservations about these newer models of NTD.[668] At the same time, the relevance of NTD motivated content removals appears to decline in importance. Today, proactive and automated, artificial-intelligence-based detection systems, such as *Google's Content ID* software for copyright infringements, or *Facebook's* software to detect terrorist content, make up over 98% of all removals on these platforms.[669]

iii. Awareness of illegal activity or information

National interpretations

Awareness of facts and circumstances from which illegal activity is apparent is another unclear and hotly debated issue.[670] For truly passive hosts there would appear to be no other way of receiving indications of the apparent illegal nature of information or conduct other than being notified of it by users or other stakeholders. According to some Member States' early interpretations, mere awareness of illegal activity would constitute objective, general knowledge and therefore not trigger liabilities. Meanwhile, the absence of awareness of facts that indicate unlawful activity is in some Member States interpreted as absence of gross negligence, and related to more specific knowledge.[671]

In an early German decision, an e-commerce marketplace was absolved from that gross negligence. The existence of past trademark violations and of general indications over the occurrence of sales of counterfeits via the platform did not constitute facts that made the existence of specific illegal activities apparent. It also precluded an obligation on behalf of the online marketplace to seek more concrete information, because this would violate

668 European Commission, 'C(2018) 1177 Final' (n 8) Recital 29, paras 25-27; Schwemer (n 660).

669 'Press - YouTube' <https://www.youtube.com/about/press/> accessed 4 June 2020; Facebook, 'Community Standards Enforcement Report - Terrorist Propaganda' (2019) <https://transparency.facebook.com/community-standards-enforcement#terrorist-propaganda> accessed 28 April 2020. This will be discussed in more detail under the private enforcement sections of the sectoral analysis in Chapter 4.

670 Directive 2000/31 (ECD) Article 14 (1) (a).

671 For example in Germany, Austria and Italy: Verbiest and others (n 315) 37–43; Kempel and Wege (n 16) 101.

Article 15 ECD.[672] This judgement was escalated up to the BGH as *Internetversteigerung II*. The BGH contrasted the earlier rulings and found that an online intermediary can be made liable for future, similar infringements under certain circumstances, such as past infringements that point towards the danger of future violations.[673]

An additional dimension is added when courts tie the question of the awareness of the intermediary over facts and circumstances pointing to illegal acts to the degree to which information is manifestly illegal. Thus, courts in France found that hate speech and racist content were more likely to provide clear indications of illegal activity. In Belgium, this was the case for child pornographic content. In Austria this also included defamatory content, according to the aforementioned EU study by *Verbiest et al*. By contrast, IP violations impose a higher barrier of manifest illegality due to the complex nature of these rights. However, in the French *Dailymotion* case of 2007, the Paris court found that the VSP's architecture and technology was aimed at maximising content sharing between users.[674] The company should have been aware that the success of its business model, which relied on maximising advertising revenue, necessarily included the sharing of copyright protected content. The court concluded that *Dailymotion* had knowledge of the fact that infringing videos would be shared via its sites. It could not offload its responsibility to the users, whom it had equipped with the means to committing these infringements.

The above rulings show the complicated and ambiguous nature of intermediaries' obligations: should an awareness of past infringements and/or manifestly illegal content constitute a reason for the intermediary to become more alert, or risk conscious? Would this then imply a higher likelihood of being aware of and discovering specific instances of unlawful activity, or should the prohibition of any "general obligation to actively to seek facts or circumstances indicating illegal activity" as of Article 15 (1) ECD, be interpreted strictly, i.e. regardless of the illegal nature and the history of infringements? Article 15 was originally put in place to protect the emerging intermediary sector from detrimental economic and legal burdens that could have endangered the open development of the internet. However, the situation had started to change towards the end of the 2010s, when some of the above rulings were made.

672 *Markenrechtsverletzung durch Onlineauktion* [2002] LG Düsseldorf 4a O 464/01 [126].

673 *Internetversteigerung II (Rolex v Ricardo.de)* (n 568) 510.

674 *Christian, C., Nord Ouest Production v Dailymotion, UGC Images* (n 196).

CJEU clarification

The CJEU's first iteration on the issue comes again from *L'Oréal v eBay*. The court clarified that awareness of facts or circumstances "on the basis of which a diligent economic operator should have identified the illegality in question" constituted actionable knowledge.[675] Failure to remove or prevent access to any unlawful information that it discovered as part of its reasonable due diligence would trigger liability. This includes investigations undertaken on the intermediary's own initiative.[676]

It is important to note that the CJEU did not go the route of previous national rulings and provide indications on the significance of the obviousness of illegality or the history of violations. Rather, it went beyond and suggested that, though passive information hosts may not have general knowledge of unlawful activity, to a diligent economic operator specific illegal acts could become apparent.[677] *L'Oréal v eBay* was the first time that the CJEU confirmed the existence of more general duties for an online platform that go beyond the reactive obligations established through NTD. The diligent economic operator principles formulated in *L'Oréal v eBay* are comparable to duties of care, which Member States may oblige hosting providers to apply under the ECD,[678] or, arguably, even broader principles of (corporate) responsibility and ethics.[679] Again, it is up to Member States to formulate these principles. Nevertheless, the diligent economic operator concept for intermediaries was taken up by the European Commission as a confirmation that voluntary proactive measures may lead to actual knowledge.[680] It was also taken over into the new (Copyright) Digital Single Market Directive (DSMD). The DSMD essentially applies diligent operator principles to evaluate online content-sharing service providers' (OCSSPs) best efforts to prevent unauthorised works being made available through their systems)).[681] National courts have also adopted this guidance, not only in the area of e-commerce and trademarks,[682] but also for cases involving defamation.[683]

---

675 *L'Oréal v eBay* (n 463) para 120.
676 ibid 122.
677 Valcke, Kuczerawy and Ombelet (n 551) 108–109.
678 Directive 2000/31 (ECD) Recital 48.
679 Valcke, Kuczerawy and Ombelet (n 551) 114.
680 European Commission, 'COM (2017) 555 Final' (n 69) 12.
681 DSMD 2019/790 Recital 66. Although the platforms covered in this provision are already outside the scope of the ECD.
682 *Maceo v. eBay International AG,* (n 578). under Chapter « Discussion »
683 *CG v Facebook* (n 625) para 72.

This is one of the more problematic aspects of the ECD's liability regime. It actually discourages platforms from (openly) engaging in voluntary measures to prevent and detect illegal content, as any failure to act expeditiously on its removal may result in liabilities. It may lead to the paradox situation that platforms are incentivised not to be too curious about their clients' activities lest they could "stumble upon" and therefore become aware of concrete incidences of unlawful activity. The introduction of the diligent economic operator concept in intermediary liability can be seen as an attempt to formulate some reasonable, positive duties in the absence of any statutory encouragement for voluntary measures, although the effects may not be the same.

The US "Good Samaritan" provisions in the CDA and the DMCA protect those intermediaries that voluntarily engage in good faith measures to prevent unlawful content against any charges for negligent behaviour.[684] However, even that provision is increasingly criticised as counter-productive when it comes to unlawful material on the internet.[685]

The *L'Oréal v eBay* ruling has also been criticised for potentially conflicting with the ECD's Article 15, which prohibits the imposition of general monitoring obligations. Intermediaries may be nudged into monitoring more broadly for illegal activity in order to be seen as diligent economic operators.[686] However, this may be too simplistic as an interpretation. Whether the broad prohibition of general monitoring obligations does indeed stand in the way of diligence principles will be discussed below.

The awareness standard of "red flag" knowledge in the US and China

In the US, the same concept of awareness of facts and circumstances exists for intermediaries under copyright law,[687] but not for violations under the CDA. It was the intention of US lawmakers to establish the existence of this awareness through a "red flag" test.[688] This test has a subjective ele-

684 47 USC § 230 (c) (2); 17 U.S.C. § 512 (g) (1).

685 Zuboff (n 5) l 2040; Danielle Keats Citron and Benjamin Wittes, 'The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity' (2017) University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2017-22 14–15 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007720> accessed 18 September 2017; Dr Melanie Smith, 'Enforcement and Cooperation between Member States' (European Parliament 2020) 32.

686 Savin (n 384) 161.

687 17 U.S.C. § 512 (c) (1) (A) (ii), (d) (1) (B) (ii).

688 'House of Representatives - Digital Millennium Copyright Act of 1998' (n 404) 53–54.

ment of establishing the concrete facts and circumstances, and an objective element that determines whether for a reasonable person acting under these subjective circumstances the unlawful activity would have been apparent. The interpretation is meant to be relatively strict, with liability limited to specific incidences of blatantly visible unlawful acts. The red flag test, it appears, establishes a higher standard of "should have known" knowledge than that of the diligent economic operator.

US Courts have indeed exercised considerable restraint in finding intermediaries liable under this test. The final judgement in *Viacom v YouTube*[689] ended a six-year litigation battle in which the entertainment giant claimed $1 billion in damages for unauthorised broadcasts of videos. *YouTube* was acquitted on all counts and held not responsible for uploads by its users, nor obliged to monitor its site for unauthorised uploads even though it had received indications that some of these could contain infringing material. Red flags would only be found in cases of blindness to specific, identifiable infringements. The court overruled an earlier judgement which had found *YouTube* liable because it was wilfully blind to specific infringing acts and aware of massive infringements on its site.[690] This narrow interpretation of a red flag is confirmed by *Corbis v Amazon*, which was about the availability of copyright infringing images through sites owned by the e-commerce giant. The court laid down that a red flag existed when the infringing nature of content would be obviously "apparent from even a brief and casual viewing" of the website. In other words, such a flag must be "brightly red indeed – and be waving blatantly in the provider's face – to serve the statutory goal of making infringing activity… apparent."[691] Indeed, such a red flag is therefore difficult to prove under US law. It depends on whether in the course of its normal business the intermediary became aware of the unlawfulness of specific acts. Meanwhile, *Corbis v Amazon* confirms that mere notifications of infringing activity would not confer knowledge of other infringements, nor that awareness of suspicious activity amounted to red flags.[692]

Chinese courts appear to apply their red flag knowledge standard in a more hawkish way.[693] Contrary to the US, this standard is seen in conjunc-

689 *Viacom International v YouTube* [2013] US District Court for the Southern District of New York No. 07 Civ. 2103, 2013 WL 1689071.
690 *Viacom 2012* (n 196).
691 David Nimmer, *Copyright: Sacred Text, Technology, and the DMCA* (Kluwer Law International 2003). In: Wang (n 504) 280.
692 Burk (n 295) 442.
693 Tao (n 506) 15–16.

tion with more expansive duty of care obligations.[694] Chinese courts have considered "should know" circumstances, such as a combination of high popularity of content (established through the number of downloads and the release date) and the way this content is sorted, recommended or commercially exploited (i.e. through advertising) as giving indications of red flags. In addition, they consider factors such as the business model, or the way the intermediary deals with infringement notices and the proactive measures it has in place. If, under the combined consideration of all these circumstances, the platform should have been aware of obviously infringing activity, or even the risk thereof, then a red flag would exist. In essence, the more a platform is involved in the hosting of highly popular and commercially valuable content, the more it is at risk of discovering red flags for unlawful activity on its site.[695] Since Chinese intermediary provisions do not have any protections against general monitoring obligations, courts have been less inhibited to considering more expansive interpretations of red flag knowledge.

III. The preventive obligations of intermediaries

The largely reactive duties of intermediaries with regards to the removal of unlawful content created conflicts early on. Once uploaded, it is notoriously difficult, if not impossible, to delete or remove information from the internet. As users can often be anonymous or easily disguise their identity, repeat uploads or sharing of banned content require little extra effort. Fighting the almost endemic repeat uploads and proliferation of unlawful content in a more effective manner would, however, imply that the reactive duties be complimented by preventive efforts. Intermediaries, as the gatekeepers to and hosts of this information are obvious targets for this, on a technical and economic level, but also on moral and legal grounds.

The ECD opens the door for courts and authorities to require online intermediaries to terminate and prevent infringements.[696] However, the scope of injunctions to prevent infringements soon turned out to be problematic in view of the limitations imposed by Article 15 ECD.

Naturally, damaged parties had an interest to ensure that information that was removed once through an NTD request did not reappear, but

694 Wang (n 504) 308.
695 ibid 284–286.
696 Directive 2000/31 (ECD) Articles 12 (3), 13 (2), 14 (3).

stayed-down permanently. This has remained one of the most difficult and seemingly unsurmountable problems until today. The legal answer to this were stay-down orders, which aim at ensuring that, once a piece of notified content was removed, it was successively blocked by the intermediary from reappearing. In addition, courts and authorities sought to widen the scope of these preventive injunctions by obliging intermediaries to not only block the same, but also similar infringing content, or even a broad, unspecified range of future infringements.[697]

Intermediaries saw themselves very soon on the defensive and claimed that these preventive injunctions conflicted with Article 15 ECD.[698] They argued that these injunctions imposed *de facto* general monitoring obligations on them, because they would force them to monitor their entire traffic to identify the content covered by the injunction. Indeed, at least in some earlier cases (discussed below), it was argued that even more specific stay-down orders would necessitate a general monitoring of traffic. On the other side, those demanding preventive injunctions reasoned that orders aimed at preventing specific content only necessitated a closely circumscribed monitoring or filtering. This would be in compliance with the ECD's Article 15 and in the spirit of Recital 47 which specified that monitoring obligations in a specific case cannot be prevented. These conflicts were addressed in Member States' courts with varying methodologies and results.

Matters were not made easier by the fact that the ECD does not define the term general monitoring. Meanwhile, content and data recognition, filtering and analytics technologies have become more effective, less intrusive and scalable, which also impacted this debate.[699]

A further point of complication is introduced by Recital 48, which gives Member States the option to require hosting providers to apply "duties of care, which can reasonably be expected from them and which are specified by national law in order to detect and prevent certain types of illegal activi-

697 As, for example, in *Scarlet Extended* (n 139).

698 On the motivations behind Article 15 ECD see above in this chapter

699 Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International BV 2017) 473–474; Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18, 82. Lorna Woods, 'The Carnegie Statutory Duty of Care and Fundamental Freedoms' [2019] Carnegie UK Trust 11 <https://www.carnegieuktrust.org.uk/publications/doc-fundamental-freedoms/> accessed 2 March 2020.

ties."[700] This requirement could, on the one hand be interpreted as conflicting with the limitations imposed by Article 15 ECD.[701] On the other hand, this passage could be seen as unwittingly causing the well-meant intention to encourage the application of more encompassing notions of responsibility to amplify the divergence between national intermediary liability practices. The tort law based negligence that underpins duty of care does not call up identical normative concepts and applications nationally. A look at the different translations of the duty of care referred to in Recital 48 may give a glimpse of this. While in German, Recital 48 refers to *Sorgfaltspflicht* (which can be literally translated into duty of care), the French version speaks of *précautions*, and the Italian version points to *dovere di diligenza* (diligence duties). For Germany, the direct link has been made between the concept of *Sorgfaltspflicht* (although referring to its iteration in the *L'Oréal v EBay* ruling),[702] and the German law "interferer liability" that has been widely applied in national intermediary liability cases.[703] For France, however, no such clear link between the concept of *précautions* and the broad formulations of the *Code Civil's* civil liability Articles 1240 and 1241 can be made. In fact, *van Dam* suggests that the French concept of *faute* in the Code Civil refers to negligence simply as a lack of a certain standard of care, but does not impose a *duty* of care.[704] The reference to *précautions* in the ECD may therefore not add any value other than 'permitting' French courts to apply their broad secondary law concepts. A similar observation can be made for Italy, where, as explained in the previous chapter, secondary liability rules are more linked to vicarious liability.

It should be noted that the difficulties of pinning down preventive duties concern mainly information hosts. However, IAPs had also been early in the focus of courts due to their central function of enabling access to the internet. Injunctions against IAPs would normally concern the disabling or filtering of locations on the internet (DNS/IP/URL based) or of content by restricting certain applications (i.e. P2P systems). Court injunctions against host providers, on the other hand, focus more on identifying and

700 Directive 2000/31 (ECD) Recital 48.

701 Gerald Spindler, Fabian Schuster and Katharina Anton (eds), *Recht Der Elektronischen Medien: Kommentar* (2. Aufl, CH Beck 2011) 1511. (see also supra fn 724)

702 *L'Oréal v eBay* (n 463) para 124.

703 Jan Bernd Nordemann, 'Haftung von Providern im Urheberrecht Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – C-324/09 – L'Oréal/eBay' GRUR 2011 977, 978–879.

704 CC van Dam, *European Tort Law* (Second edition, Oxford University Press 2013) paras 302–1.

preventing unlawful content hosted on their sites. For the legal argumentation at hand the difference shall not be important as the basic conflict between specific and general infringement prevention poses the same normative legal problems.

a. National case law

i. France

In the French cases brought against *Google Video* in 2007[705] it was found that the company had an obligation to monitor and prevent every re-upload of content that had been previously notified. *Google* was charged with copyright violation for every upload that re-occurred. It had originally argued that for each (re-)upload a separate NTD request would have to be filed. Meanwhile, *Dailymotion* was explicitly denied the protections of Article 15 ECD because, according to the court, it had induced its users to uploading infringing material. This meant the VSP had actual knowledge of its site being used for infringing activities and therefore needed to monitor its traffic for illegal content before upload by its users.[706] French courts continued to apply notice-and-stay-down obligations in a number of cases directed at *Google Video*. The company was denied the protections of the ECD because it failed to disable future uploads of once notified copyright protected content.[707]

In a trademark case that set *eBay* against *L'Oréal* a Paris court found that the marketplace had fulfilled its obligations as an intermediary, which consisted of ensuring that its activities did not facilitate illicit acts. These activi-

705 *Christian, C., Nord Ouest Production v Dailymotion, UGC Images* (n 196). *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud v Sté Google Inc et AFA* (2007) (Unreported) (Tribunal de grande instance de Paris).

706 *Christian, C., Nord Ouest Production v Dailymotion, UGC Images* (n 196) see under « DISCUSSION - Sur la nature de l'activité exercée par la société Dailymotion et sa responsabilité ».

707 Catherine Jasser, 'Recent Decisions of the Paris Court of Appeal: Towards an Extra Duty of Surveillance for Hosting Providers?' (*Kluwer Copyright Blog*, 29 March 2011) <http://copyrightblog.kluweriplaw.com/2011/03/29/recent-decisions-of-the-paris-court-of-appeal-towards-an-extra-duty-of-surveillance-for-hosting-providers/> accessed 17 February 2020. Aleksandra Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: From Concepts to Safeguards* (Intersentia 2018) 234–235. See for example: *Google Inc v Les Films de la Croisade, Goatworks Films* (2010) (Unreported) (Cour d'appel de Paris Pôle 5, chambre 2).

ties consisted, amongst others, in contractual clauses, information targeted at advertisers and sellers, notification tools for unlawful content, an IP right protection programme (*VeRo*), dedicated staff and key word searches aimed at identifying counterfeit products.[708] Any further obligations would be in conflict with Article 15 ECD. The ruling implies that certain proactive prevention measures, that may even go beyond repressing specific repeat infringement, were seen as adequate and in compliance with Articles 14 and 15 ECD. From 2012, this practice however was somewhat qualified when the French Supreme Court ruled that in order to "prevent any new upload of the infringing videos, without even being informed of it by another notification, which is nevertheless required for them [Google] to be effectively aware of its illegal nature" would amount to a general obligation to monitor for illicit content.[709]

ii. Italy

Italian courts initially offered differing readings of the interplay between authorised specific and prohibited general preventive obligations.[710] In a legal battle stretching several years between *Google's YouTube* service and *Delta TV*, a Turin court confirmed in 2017 an earlier decision by another Italian court.[711] It obliged the VSP to prevent any future uploads of copyright infringing content that it had removed due to earlier NTD requests by deploying its *Content ID* software. As a "new generation" hosting service it needed to take over enlarged responsibilities, which would be in line with the "duty to act" in order to prevent illegal activities, provided for in Recital 40 ECD.[712] By contrast, in a parallel ongoing dispute between *RTI*, a private Italian broadcaster, and *Yahoo!*, the Milan court overturned previous instances and found that *Yahoo!* was not obliged to ensure that once removed unlawful content stayed down as this would require it to monitor

708 *L'Oréal SA c eBay France SA* (n 565).
709 *Google Francev Bac films* [2012] Cour de cassation, Première chambre civile 11-13.669, FR : CCASS : 2012 : C100831; (translation by author) see also: Amélie Blocman, 'Pas d'obligation générale de surveillance du réseau, rappelle la Cour de cassation' [2013] iris plus.
710 Giancarlo F Frosio, 'The Death of No Monitoring Obligations' (2017) 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 199, 205–206.
711 *Delta TV v Google and YouTube* (n 622).
712 Frosio, 'The Death of No Monitoring Obligations' (n 709) 206.

its site in a general fashion.[713] This decision was then overturned by the Italian Supreme Court, which found that stay-down obligations were specific and therefore in line with the provisions of the ECD, and did not mean the VSP needed to monitor its service in a general way.[714] In Italy, dynamic blocking injunctions have also been successful. For example, in 2017, Italian publisher *Mondadori* succeeded in bringing action against several internet service providers for copyright infringement and required them to go beyond blocking the domain names identified in the original injunction.[715] The perpetrating platform changed its domain names dynamically and redirected traffic to the servers where infringing material was hosted, a common practice to subvert blocking activities. *Mondadori* requested that the providers identify and block all future domain names (hence dynamic blocking) that directed to the infringing platform in question. In this decision, the eligibility of these measures was judged mainly from the IP Rights Enforcement Directive (IPRED), and especially the guidance document of the European Commission, which will be discussed later in the copyright section of Chapter 4.[716] However, the court also found that the dynamic injunction did not constitute a general monitoring obligation, if the right holder provided a list specifying the new domain names that needed to be blocked.[717]

---

713 *Yahoo! Italia S.r.l and Yahoo! Inc, v Reti Televisive Italiane S.pA* (2015) (Unreported) (Court of Appeal of Milan). Mario Berliri, 'The Court of Appeal of Milan Rules on Yahoo's Liability with Respect to Copyright Infringement' (*Global Media and Communications Watch*, 25 February 2015) <https://www.hlmediacomms.com/2015/02/25/the-court-of-appeal-of-milan-rules-on-yahoos-liability-with-respect-to-copyright-infringement/> accessed 18 February 2020.

714 *Reti Televisive Italiane SpA v Yahoo! Inc and Reti Televisive Italiane SpA v Yahoo! Inc.* (n 621); Rosati, 'Italian Supreme Court Clarifies Availability of Safe Harbours, Content of Notice-and-Takedown Requests, and Stay-down Obligations - The IPKat | Diigo' (n 621).

715 *Arnoldo Mondadori Editore SPA, v Fastweb SPA and others* [2018] Tribunale di Milano 51624/2017. In: Eleonora Rosati, 'Milan Court Issues Dynamic Blocking Injunction against Italian ISPs - The IPKat' (*The IPKat*, 25 August 2018) <https://ipkitten.blogspot.com/2018/08/milan-court-issues-dynamic-blocking.html> accessed 18 February 2020.

716 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'.

717 Rosati, 'Milan Court Issues Dynamic Blocking Injunction against Italian ISPs - The IPKat' (n 714).

iii. Germany

German courts developed rather intricate ways of defining the proactive obligations of internet intermediaries. The *BGH* confirmed the legality of stay-down orders as early as 2004 in *Internetversteigerung I*, and then later in *Internetversteigerung II and II in* 2007 and 2008.[718] In these cases, the *BGH* found that not only did e-commerce marketplace *Ricardo.de* (and later *eBay*) had to ensure the stay-down of specific offers of trademark infringing *Rolex* watches. Moreover, following the specific infringement notifications, it had a duty to prevent the offer of all clearly noticeable trademark infringements relating to the *Rolex* brand in general, including associated brands and model numbers.[719] This duty is part of the German civil law doctrine for intermediaries known as *Störerhaftung ("interferer liability")*.[720] The *BGH* confirmed that this preventive activity could involve the use of automated means, such as filter software, which detected, with the help of specific search criteria, potentially infringing offers. These would need to be verified manually.[721] Possible indicative criteria for violations of the claimant's brand could be price points or concrete indications that the products in questions were imitations. These duties of care were acceptable as long as they did not endanger the business model of the marketplace operator.

Commentators had initially seen this ruling as in conflict with Article 15 ECD, because these relatively broad duties risked creating a general surveillance infrastructure.[722] The BGH toned down its approach somewhat in *Kinderhochstühle I*. This case dealt with the counterfeit sales of baby high chairs via the *eBay* marketplace. *EBay* had checked the product images of over 6,400 alleged counterfeit offers on its site by non-automated means to find less than 0.5% of those offers actually infringing.[723] The *BGH* ruled that imposing these measures was disproportionate and went beyond a rea-

---

718 *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).

719 *Internetversteigerung III (Rolex v Ricardo.de), Az. I ZR 73/05* (n 568) para 55.

720 Urs Verweyen, 'Grenzen der Störerhaftung in Peer to Peer-Netzwerken' [2009] MMR 590, 590. This duty of care is called reasonable due diligence ("zumutbare Prüfpflicht").

721 *Internetversteigerung II (Rolex v Ricardo.de)* (n 568) 47.

722 Gerald Spindler, 'BGH-Urteil (U. v. 19.4.2007 - I ZR 35/04) Internetversteigerung II - Anmerkung' [2007] MMR 511; Nordemann (n 702) 980.

723 *Kinderhochstühle im Internet, I ZR 139/08* [2010] MIR 122010 (BGH) [41].

sonable duty of care as it endangered the company's business model. In the absence of any reliable automated means to filter for infringing products, the intermediary was not required to do more. The BGH also considered the fact that the brand owner was given the opportunity to search for infringing offers through participation in *eBay's VeRo* programme. Under these circumstances, it was not justified to ask the platform operator to engage in more onerous preventive duties than the brand owner. It has been argued that, on a practical level, this balance may not hold for other areas of unlawful content or activity (outside trademarks), such as defamatory or copyright infringing material.[724] The application of the horizontal liability principles on different areas of unlawful content shall be discussed in the next chapter.

Meanwhile, in the area of trademarks, the use of automated image and text recognition software, targeted at preventing infringements similar to already notified content seems to have entered standard reasoning of German courts. It includes limited manual checks, mainly aimed at updating filter software. The intermediary would, however, be protected against identifying infringements that are based on substantial variations in text or images and subsequent failure of the filtering software to recognise the violation. Such violations would have to be notified to the intermediary first.[725]

This line of argument was applied in copyright disputes between rightsholders and platforms, such as the aforementioned *YouTube v GEMA* saga. Here, the use of the *Content ID* file recognition software, supplemented by manual checks on the part of the intermediary, was explicitly seen as belonging to the mandatory duty of care of *YouTube*. This development is a result of similar case law adjustments over the previous years, which saw a move from more onerous manual and automatic filtering duties, although in the area of file sharing,[726] to rejecting the necessity of excessive manual checks in order to prevent future infringements.[727] Considering defamatory comments, search engines would also be subject to reasonable preventive measures once they were notified and had received proof of unlawful comments. However, given the importance of search engines for the opera-

724 Gerald Spindler, 'Präzisierungen Der Störerhaftung Im Internet Besprechung Des BGH-Urteils „Kinderhochstühle Im Internet"' [2011] GRUR 101, 107.

725 *Beeinträchtigung der Herkunftsfunktion einer Marke trotz Fälschungshinweises (Parfume Made in China)* (n 587) paras 83–84.

726 *Shareboster II* [2009] OLG Hamburg 5 U 111/08, openJur 2009, 1105.

727 *RapidShare II* (n 615).

tion the internet, preventive duty of care measures would need to be decided on a case-by-case basis.[728]

iv. UK

The approach to balancing the proactive duties of internet intermediaries is yet different in the UK. In *L'Oréal v eBay*, the existence of a filtering programme could not be counted against the intermediary and they could not be obliged to do more by law. However, the UK court was unclear about the remit of the measures *eBay* could be forced to take according to Article 11 IPRED with regards to preventing future infringements and in light of the limitations imposed by Article 15 ECD. It asked the CJEU for guidance, which eventually resulted in a key ruling, discussed above and below.[729]

By contrast, the UK is considered the jurisdiction within the EU that has most widely adopted live (and dynamic) web blocking orders into practice.[730] In *Newzbin,* the High Court endorsed the use of targeted and narrow web blocking orders against IAP *British Telecom* in order to block access to the sites and services of *Newzbin*. The site had already been charged previously with giving access to and hosting copyright infringing content. The measures were found both as in compliance with Article 15 ECD and as proportional with regards to balancing copyright with the fundamental rights of freedom of expression of *Newzbin*, its users and *BT*.[731] They subsequently led to a wave of similar requests by rightsholders. Eventually, they also covered trademarks.[732] Dynamically modified live blocking orders are now also a common practice in the fight against live streaming of popular sports events, such as football matches.[733] In essence, rightsholders have

728 *Haftung des Suchmaschinenbetreibers für geschlossene rechtswidrige Äußerungen* [2014] LG Hamburg 324 O 660/12, openJur 2014, 26809 [87–88].
729 *L'Oreal SA v. eBay International AG* (n 563) paras 375, 464–465.
730 Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 283.
731 *Newzbin* (n 638) 161–162, 199–201.
732 *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors [2016]* [2106] England and Wales Court of Appeal (Civil Division) A3/2014/3939 & A3/2014/4238, EWCA Civ 658.
733 *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] 2017 EWHC 480 Ch (England and Wales High Court (Chancery Division)).

with success tried to force ISPs to adopt a filtering and blocking technology called *Cleanfeed*, developed by *BT*. *Cleanfeed* was originally set up to act on child pornographic content identified by the *Internet Watch Foundation (IWF)*.

Much of the national jurisprudence by EU Member States, decided after 2011, appears to draw on the guidance given in the first intermediary liability rulings of the CJEU.[734] Yet, despite the supposedly clarifying character of the CJEU's jurisprudence, the above trends still show that national courts continued to come to different interpretations on the scope of proactivity that can be required of internet intermediaries.[735] This can be attributed to several, interdependent reasons. First, different legal traditions may have different impacts on how the proactive obligations for (internet) intermediaries under criminal and civil provisions are interpreted. Secondly, the CJEU's interpretation of EU law in preliminary rulings is handed back to national courts for implementation. As part of this procedure, the CJEU often requires a separate assessment of the matter based on the facts at hand, which may limit the unifying character of these rulings, given differing national legal traditions. Thirdly, the fact that even within Member States decisions may vary (e.g. France, Italy), testifies to the technically complex and fast-moving nature of internet intermediary liability as well as the mounting pressure on courts and policymakers to act in the face of the aggravating problem of unlawful content.[736]

Preventive obligations outside the EU

In the US, the DMCA and the Lanham Act provide for injunction aimed at preventing repeat or future infringements in the area of copyright and trademarks.[737] In the area of copyright, intermediaries are also barred from interfering with any technical measures used by rightsowners to identify and protect copyrighted works. Meanwhile, no such legal provisions exist for other areas of unlawful online content covered by the CDA. This statue

734 Such as *Google France v Louis Vuitton* (n 155); *L'Oréal v eBay* (n 463); *SABAM v Netlog* (n 460); *Scarlet Extended* (n 139).

735 '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' (Conseil Superieur de la Propriete Litteraire et Artistique (CSPLA), Ministère de la Culture 2017) 9 <https://perma.cc/5A6F-4VDJ> accessed 21 April 2021.

736 Van Eecke (n 16); Valcke, Kuczerawy and Ombelet (n 551).

737 17 U.S.C. § 512 (i) (1) (A); 15 U.S.C.§ 1114 (2) (B).

does not allow for any remedies against interactive computer services.[738] In addition, the DMCA, like the ECD, shields intermediaries from any obligation to proactively monitoring its service or seeking facts indicating infringing activity.[739]

An obligation to prevent repeat infringements in the area of IP is the maximum that US courts have been requiring from intermediaries as regards proactive measures.[740] The "Good Samaritan" protections merely encourage the development of self-regulatory and voluntary enforcement practices between platform operators and rightsholders.[741] Content stay-down obligations have so far not been enforced against intermediaries in the US. However, pressures exist to introduce these kinds of obligations, especially in the area of copyright.[742]

Stay-down orders and obligations to monitor more proactively for infringing activity have, however, been imposed throughout other jurisdictions in the world, such as Australia, India, China, Japan or South Korea, to name but a few.[743] With regards to India and China, this can partly be explained by an absence in the law of any Article 15 ECD style limitation that prohibits general monitoring duties. As detailed above, there has been a focus on developing more proactive, duty of care style, monitoring obligations in these jurisdictions. This concerns both once notified infringements (stay-downs), but also broader efforts to prevent specific types of infringements. These trends can now also be observed worldwide across virtually all types of unlawful content and activity.[744]

738 Mehra and Trimble (n 385) 104.
739 17 U.S.C. § 512 (m).
740 *Perfect 10, Inc v CCBill, LLC* [2007] 9th Cir 04-57143, 04-57207, 488 F3d 1102 [27–29]; *Corbis Corp v Amazon Inc* [2004] US District Court, WD Washington (Seattle) No. CV03-1415L., 351 F.Supp.2d 1090 [1102–1103].
741 Rich and Ho (n 602) 8–9.
742 Evan Engstrom and Nick Feamster, 'The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools' (Engine 2017) 8–10 <https://www.engine.is/the-limits-of-filtering> accessed 3 March 2020; Urban, Karaganis and Schofield (n 661) 60–62.
743 Dan Jerker B Svantesson, 'Internet & Jurisdiction Global Status Report 2019' (Internet & Jurisdiction Policy Network 2019) 73–128, 142–146.
744 ibid 142.

b. CJEU and ECtHR case law

i. L'Oréal v EBay (C-324/09)

The problem of the permissible proactive duties of internet intermediaries under the ECD was addressed for the first time in *L'Oréal v EBay*. This case confirmed that an injunction against an intermediary to prevent future intellectual property infringements must not result in the monitoring of all content. This would be irreconcilable with the ECD and IPRED Article 3. The latter stipulates that any measures and remedies to protect IP rights must be proportionate, provide for safeguards against abuse and must not create barriers to trade. However, these measures must also be effective and dissuasive. If the hosting provider failed to take on its own initiative measures aimed at preventing infringements of the same kind by the same seller, a court would have the power to impose such measures.[745] This is somewhat commensurate with earlier German case law in e.g. *Internetversteigerung I – II*. The CJEU can be credited for confirming that hosting providers are obliged to be more than just reactive notice recipients when it comes to preventing unlawful activity. Some commentators have seen a possible contradiction between Article 15 and Recital 48 ECD. The latter gives Member States leeway in imposing reasonable duties of care on hosting providers.[746] However, *L'Oréal v eBay* confirmed at the highest EU level that stay-down orders did not amount to a general monitoring duty on behalf of the intermediary. Whether a permissible proactive duty went beyond stay-down orders is a matter for interpretation of the term "the same kind of infringements." That interpretation however is up to national courts. As shown above, this has indeed led to differing approaches and interpretations. Arguably, the clarification by the CJEU therefore opened up new threats of national diversion in the conditions that govern intermediary liability.

The CJEU also said in *L'Oréal v eBay* that an e-commerce marketplace may be ordered to make identification of its customer-sellers easier so that damaged parties can profit from their right to an effective remedy. This should be balanced with other rights as laid down in *Promusicae*, an earlier

745 *L'Oréal v eBay* (n 463) para 141.

746 Rosa Julià-Barceló and Kamiel J Koelman, 'Intermediary Liability in the E-Commerce Directive: So Far so Good, but It's Not Enough' (2000) 16 Computer Law & Security Review 231, 232. Spindler, Schuster and Anton (n 700) 1511; Lodder and Murray (n 448) 53.

CJEU ruling about the right of copyright holders to receive personal data from an IAP about users that allegedly infringed copyright.[747] This can also be interpreted as justifying additional due diligence measures that may be required from platforms.[748] Moreover, the term prevention of further infringements "by the same seller"[749] implies a certain amount of monitoring on behalf of the platform of parties that are repeatedly found to engage in unlawful acts. This would suggest that customer-sellers on online marketplace would need to go through a verification or identification process. Allowing anonymity with regards to the economic activity of selling could arguably be interpreted as a lack of diligence on behalf of the marketplace operator, according to this ruling. Finally, *L'Oréal v eBay* introduced the diligent economic operator principle. According to this, a hosting provider, in this case an online marketplace operator, could lose its immunity protections under Article 14 (1) ECD if it ignored indications of illegal activity that a diligent economic operator should have been aware of. This includes the receipt of notifications of illegal activity or information, but also situations where the marketplace had uncovered such unlawful activity or information following its own proactive investigation.[750] With the diligent economic operator concept and the requirements to prevent future infringements of the same kind by the same seller and make identification of customer-sellers easier, the CJEU formulated for the first time duties of care style responsibilities for online intermediaries that go beyond pure reactive obligations. It should be remembered that the ECD gives Member States the option of applying duties of care through national legal systems.[751] In this respect, *L'Oréal v eBay* is probably one of *the* landmark cases in EU intermediary liability jurisprudence.

ii. Scarlet Extended (C-70/10) & Netlog (C-360/10)

While *L'Oréal v eBay* explored the permissible scope of specific, preventive injunctions and proactive duties of intermediaries in the light of the prohi-

747 *L'Oréal v eBay* (n 463) paras 142–143; *Promusicae* (n 140).
748 Carsten Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet: Adopting the Anti-Money Laundering Framework to Online Platforms' (2018) 26 International Journal of Law and Information Technology 226, 243.
749 *L'Oréal v eBay* (n 463) para 141.
750 ibid 122.
751 Directive 2000/31 (ECD) Recital 48.

bition to impose general monitoring obligations, *Scarlet Extended* and *Netlog*[752] clarified the reach of broader preventive injunctions under Article 15 ECD. The Belgian association of music authors and rightsholder (SABAM) filed charges against IAP *Scarlet* and the social networking site *Netlog*, a hosting provider.

SABAM tried to prevent alleged copyright infringements of musical works in its repertoire committed by users of both companies' services by imposing an obligation on both intermediaries to prevent the unauthorised making available of works. In *Scarlet Extended*, the rights management organisation *SABAM* argued that the IAP was best placed to take technical measures to stop copyright infringements of its subscribers through the use of P2P services. *SABAM* first successfully achieved an order by a Belgian court that *Scarlet* filter and block on a permanent basis all P2P traffic by its users which was aimed at sharing works in SABAM's repertoire. The IAP, however, appealed claiming that such an order resulted in a *de facto* general monitoring obligation because it would require it to screen its entire traffic for P2P transmissions. In addition, this measure was not proven to be effective and would negatively impact the company's network operation. Furthermore, it would be in contravention of Article 15 ECD and, lastly, violate EU law on the protection of personal data and the secrecy of communications.[753]

In *Netlog*, *SABAM* demanded that the social network prevent its users to share works under the license of SABAM and asked for damages for any delays in complying with this order. Similar to *Scarlet Extended*, *Netlog* argued that this would result in a *de facto* general monitoring of its users' activities and breach the same EU law provisions as detailed in *Scarlet Extended*.

Both cases were argued by the CJEU essentially on the same lines, but concerning two types of intermediaries: *Scarlet*, a mere conduit, and *Netlog*, a hosting provider. The referring questions of the Belgian courts went beyond asking for guidance on whether the measures required by *SABAM* were in contravention of Article 15 ECD. They also asked whether they were permitted under the Infosoc Directive and IPRED, read in conjunction with the ECD, data protection, secrecy of communication legislation

752 *Scarlet Extended* (n 139); *SABAM v Netlog* (n 460).
753 *Scarlet Extended* (n 139) paras 23–26.

and EU Fundamental Rights.[754] The Infosoc Directive and IPRED allow for the imposition of injunctions against intermediaries, but require at the same time that any such measures are effective, proportionate and dissuasive, and, regarding IPRED, are not unnecessarily complicated or costly.[755]

In both cases the CJEU ruled that *SABAM's* orders would have required the IAP (*Scarlet*) to filter all electronic communications, and the hosting provider (*Netlog*) to filter all information stored on its service. These orders would have applied indiscriminately to all users, on a preventative basis, at the exclusive expense of the service and for an unlimited period. The CJEU judged that this would amount to an obligation to monitor its traffic on a general basis. They were therefore in violation of Infosoc Directive, IPRED, the applicable fundamental rights and Article 15 ECD. In the cases at hand, the fundamental rights of the freedom to conduct a business, the right to protection of personal data and the freedom to receive or impart information were outweighing the right to intellectual property.[756]

Scarlet Extended and *Netlog* defined the limits of Article 15 ECD[757] and also performed a clarifying balancing exercise between EU law and fundamental rights, given the specific filtering injunctions demanded by rightsholder *SABAM*. This ruling provided useful guidance on when a preventive injunction would generate effects that are in violation of EU law. It also implied, however, that adequately designed filtering injunctions may indeed be possible. This issue was first dealt with by the CJEU in *UPC Telekabel.*[758] It is worth mentioning, however, that the CJEU ruled in that case, which involved specific blocking injunctions against Austrian IAP *UPC*

754 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 (OJ L 281) 46; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 (OJ L 201) 58; European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 Articles 8 & 10.

755 Directive 2001/29 (Infosoc Directive) Article 8; Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights Articles 3, 11.

756 *Scarlet Extended* (n 139) paras 53–54; *SABAM v Netlog* (n 460) paras 51–52.

757 Stalla-Bourdillon, 'Sometimes One Is Not Enough! Securing Freedom of Expression, Encouraging Private Regulation, or Subsidizing Internet Intermediaries or All Three at the Same Time: The Dilemma of Internet Intermediaries' Liability' (n 484) 173.

758 *UPC Telekabel Wien GmbH v Constantin Film Verleib GmbH, Wega Filmproduktionsgesellschaft mbH, C-314/12* [2014] EU:C:2014:192 (CJEU).

Telekabel, solely in respect of the Infosoc Directive, and did not follow the AG Opinion's deliberations, which included an assessment of the compatibility with Article 15 ECD.[759]

This opens the question whether a proportionality assessment involving fundamental rights needs to be done in the context of Article 15 ECD. Traditional reading of *Scarlet Extended* and *Netlog* sees Article 15 ECD strongly impacted by a fair balancing exercise of fundamental rights.[760] However, despite of the references between Infosoc, IPRED and the intermediary liability provisions of the ECD, the actual fundamental rights balancing exercise is conducted in the context of the proportionality provisions of IPRED's Article 3 (1).[761] This makes sense as any balancing exercises pertaining to the prevention of certain types of unlawful content should be made primarily with regard to the fundamental right attached to that content,[762] and not in respect of a broad, horizontal prohibition of general monitoring. Concerning IP rights, the IPRED Guidance confirms that the act of general monitoring prohibited by Article 15 would also fail the proportionality requirements of IPRED's Article 3 (1). Therefore, Article 15 does not seem to play a direct role, or indeed be necessary for an effective fundamental rights balancing that assesses the scope of injunctions.[763] The question is then, if the absence of Article 15 would prevent a successful fundamental right balancing exercise also beyond the area of IP rights. In addition, if a court's balancing exercise would find that more proactive prevention measures are justified under certain circumstances, e.g. facilitat-

759 *Opinion of Advocate General Cruz Villalón UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, C-314/12* [2011] EU:C:2013:781 (CJEU) [77–78]. This judgement will also be dealt with in the Chapter on the interface between copyright and intermediary liability. (p.xxx)

760 Giovanni Sartor, 'Providers Liability: From the ECommerce Directive to the Future - IP/A/IMCO/2017-07' (2017) 17–18.

761 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 230. *Scarlet Extended* (n 139) paras 41–53, 48; *SABAM v Netlog* (n 460) paras 39–51, 46.

762 Such as the IPRED 2004/48 for IP rights, and, in addition, Infosoc 2001/29 for copyright, or, for incitement to violence by national and EU law (e.g. 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)

763 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) 16–21.

ed by technology, then Article 15 ECD could theoretically still prevent this outcome.[764]

While it is not contested here that excessively broad, preventive filtering obligations are likely to violate fundamental rights, it is suggested that the ECD's Article 15 is not needed for an effective proportionality assessment. As demonstrated by the national case law, the problem of clearly distinguishing between prohibited general and permitted specific monitoring obligations has persisted to this day, despite the clarifications that the CJEU was supposed to give.

Problems with defining general monitoring at a technical level

The approaches in *Scarlet Extended* and *Netlog* imply that, in light of technological improvements in filtering and content recognition, preventive injunctions that are seen unfeasible at a certain point of time, could be considered proportionate in the future. Filtering technologies are now used more widely by online intermediaries, making content checking less costly and intrusive.[765] At the same time, these technologies have improved in accuracy and processing capacity.[766] Less intrusive filtering methods, such as shallow packet inspection, could potentially lie outside the scope of general monitoring.[767] Monitoring, in this context, denotes the act of proactively analysing user activity and content in search for any unlawful information or activity. Filtering systems partly use the results of monitoring in that they act on the identified content by either blocking or removing it. Filtering can be done by humans or through automated sys-

764 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 230.

765 See for example the development of private and public content recognition technologies, such as *Google's ContentID*, Mircosoft's *PhotoDNA*, British telecom's *Cleanfeed* system, the *AudibleMagic* or INA Signature the French Institut National de l'Audiovisuel Institut National de l'Audiovisuel, 'Ina-Signature : Protégez et Gérez Vos Contenus' <https://www.ina-expert.com/content/download/2103/44165/version/latest/file/1> accessed 5 March 2018. There are also a number of solutions by other companies targeted at helping rightsowners to identify copyright protected content on platforms, offered by e.g. Gracenote or MarkMonitor.

766 Sartor (n 236) 63. An overview of the content recognition solutions in the area of terrorist content and copyright protection will be given in Chapter 4.

767 Angelopoulos (n 30) 473–474.

tems, while monitoring is ensured through technical tools.[768] Algorithmic decision making is now routinely used by online platforms in both the distribution and the monitoring and filtering of internet content. This does, however, not mean that personal data will necessarily be processed. For example, a system that just matches content against a database of hashes, embedded metadata or watermarks does not need to analyse underlying user details or activity data.[769] The EU itself has suggested that filtering technology that is absolutely effective and available at no cost would make Article 15 unnecessary.[770] In the end, a lot depends also on defining "general monitoring", which, unfortunately, the EU lawmaker has not ventured to do. Meanwhile, the CJEU has also not established any clear methodology to distinguish lawful, specific prevention from prohibited general monitoring.[771] The lack of clarity on this has been noted many times.[772] This contributes to rendering Article 15 problematic and potentially less relevant in its application today.

iii. Mc Fadden (C-484/14)

This case focussed on the permissible scope of measures taken by a public Wi-Fi operator to prevent and deter copyright infringing activities by its users over its network.[773] The operator was a shop owner who ran a Wi-Fi network that gave free and unprotected internet access to people in the vicinity of the shop. A user of this free network committed copyright infringing acts by making music available free of charge to the general public. The rightsholder notified the violation to the Wi-Fi operator and subsequently filed claims for damages, an injunction against the infringement and reimbursement of notice costs. The operator, *Mc Fadden*, claimed exemption from liability on the grounds of Article 12 (1) ECD, as a mere conduit for internet access.

---

768 C Angelopoulos and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (Institute for Information Law (IViR), University of Amsterdam 2015) 6–9.

769 Woods, 'The Carnegie Statutory Duty of Care and Fundamental Freedoms' (n 698) 11; Edwards and Veale (n 698) 82–83.

770 European Commission, 'SEC(2011) 1641 Final' (n 11) 50.

771 Sartor (n 236) 60.

772 Nolte and Wimmers (n 551) 21–23. Friedmann (n 16) 148, 152–155; Valcke, Kuczerawy and Ombelet (n 551) 109–110; Angelopoulos (n 30) 100–107.

773 *Mc Fadden* (n 139).

The CJEU was asked first for confirmation whether the Wi-Fi operator was indeed a mere conduit under the ECD's Article 12, and secondly, whether it was obliged to prevent future infringements of the work in question. The court was also asked about the adequacy of certain measures to prevent such infringements, notably: the termination of connections; installing password protected access; and monitoring all traffic via the network. The latter measure was predictably found to be in violation of Article 15 (1) ECD. Meanwhile, requiring the Wi-Fi operator to terminate the connection was deemed a disproportionate interference with the operator's business compared to the copyright interest at stake. Password protection of access to the Wi-Fi service was, however, deemed an adequate means. It would force users to reveal their identity and was therefore more likely to be an effective deterrent against unlawful use of the service.[774]

With this ruling the CJEU confirmed the validity of preventive measures, such as customer identification, as adequate for the prevention of unlawful activity, at least where intellectual property rights are concerned. It also provided some indication on the preventive measures that an IAP could be expected to take under the ECD. This can be contrasted to the ruling in *UPC Telekabel*, which justified the scope of preventive, blocking injunctions solely through the Infosoc Directive 2001/29. Taken together with the ruling in *L'Oréal v eBay*, this can be seen as a further step to formulating reasonable duty of care requirements for online intermediaries for certain kinds of unlawful content and activity.[775]

iv. The ECtHR rulings in Delfi v Estonia & MTE v Hungary

While the European Court of Human Rights' (ECtHR) jurisprudence is not binding for the CJEU, the ECtHR still rules on the European Convention of Human Rights (ECHR) to which all EU Member States have acceded. The provisions of the ECHR are recognised as general principles of EU law[776] and the CJEU has also acknowledged the ECHR as guidelines in the application of EU law.[777] The ECtHR may therefore bring cases against EU

774 ibid 90–98.

775 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 243–244.

776 Treaty on European Union (2007) Article 6 (3).

777 *J Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities, C-4/73* [1974] EU:C:1974:51 (CJEU) [13]. In: Alina Kaczorowska, *European Union Law.* (Taylor and Francis 2013) 414.

Member States when they apply EU law and the CJEU does consider the rulings of the ECtHR.

Delfi[778] is a popular Estonian online news portal which offered its users the opportunity to comment anonymously on the news articles published on its site. One news article attracted a series of defamatory and insulting comments from readers against which the addressee of these comments filed an NTD request and claimed damages. While *Delfi* took down the abusive comments immediately, it refused to pay the damages. After regional and appeals courts in Estonia classed *Delfi* as an editor and ordered it to pay the damages, and after the Estonian Supreme Court refused to hear the case, the company went to the ECtHR claiming violation of its right to freedom of press and expression. Although the ECtHR did not come down decisively on *Delfi's* role as a provider of a comments function, it distinguished *Delfi* from bulletin boards or social media platforms. Due to its size, its editorial ownership of the news articles and the economic interest in providing reader comments, its role was more seen as that of an editor.[779] Despite of this, the ECtHR recognised the auxiliary character of *Delfi's* comments function. The judges conceded that its duties and responsibilities regarding that comment function may be different from that of a traditional publisher.[780] This is a useful analysis. It somehow sidelines the more cumbersome, and increasingly artificial, distinction between active and passive intermediaries of the CJEU and acknowledges the more differentiated role of internet intermediaries. In a certain sense, this assessment can be seen as coming close to the "active intermediary" standard developed by Italian courts.

The ECtHR considered the economic interest of the news portal and the measures that *Delfi* had in place to moderate and prevent certain types of comments. Notably, it had put in place terms and conditions, a notice-and-takedown system, automatic word filters and editorial actions by portal administrators.[781] However, despite of this, it noted, *Delfi* still failed to limit the dissemination of hate speech and speech inciting violence. Given the severity of comments at issue *Delfi* needed to do more to prevent and remove obviously unlawful comments. The need to be more proactive in this matter outweighed concerns over the protection of the fundamental

778 *Delfi AS v Estonia* [2015] ECtHR (Grand Chamber) 64569/09.
779 ibid 110–117.
780 ibid 113.
781 ibid 155.

right to freedom of speech.[782] The judgement was widely criticised for putting an undue weight on the policing role of intermediaries to the detriment of freedom expression.[783] Others speculated that the same outcome would have been reached had the case been judged by the CJEU under the ECD's liability regime. *Delfi* would likely have been found falling foul of the diligent economic operator standard.[784] If the latter is true, then the *Delfi* judgement offers a useful mini step towards establishing a standard of responsibility for comments functions of commercial news portals *vis-à-vis* defamatory speech.

The ECtHR applied this approach in *MTE*,[785] which concerned the alleged failure of a non-commercial, self-regulatory body of Hungarian internet content providers and the consumer protection section of a commercial news portal to remove and prevent defamatory speech. Both parties appealed a ruling by the Hungarian courts that allegedly deprived them of their intermediary liability protections. The ECtHR first found that the comments in question were not obviously unlawful. The comments also concerned the commercial reputation of companies as opposed to the personal reputation of private individuals in *Delfi*. In this context, the NTD system of the applicants, their terms and conditions and the employment of content moderators was sufficient to afford them protection against liability for comments by users.[786] By not taking these circumstances into account and by failing to perform a balancing exercise, the domestic courts had violated the applicants' freedom expression, guaranteed by Article 10 of the ECHR.[787] This ruling shows the malleability of due diligence obligations depending on the nature of comments and the character of the intermediary involved. Specific proactive monitoring, seen appropriate for the *Delfi* portal, may not be adequate for other types of content and intermediaries.

782 Valcke, Kuczerawy and Ombelet (n 551) 152–162.
783 Frosio, 'The Death of No Monitoring Obligations' (n 709); Martin Husovec, 'General Monitoring of Third-Party Content: Compatible with Freedom of Expression?' (2016) 11 Journal of Intellectual Property Law & Practice 17.
784 Valcke, Kuczerawy and Ombelet (n 551) 113.
785 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu zrt v Hungary* [2016] ECtHR (Fourth Section) 22947/13.
786 ibid 81.
787 ibid 88.

v. Eva Glawischnig-Piesczek v Facebook Ireland (C18/18)

In this case, brought against *Facebook*, the CJEU had the opportunity to refine its jurisprudence on the scope of preventive activity that is allowed under the ECD.[788] It was asked whether the world's largest online social network could be compelled to identify and delete defamatory comments that were posted repeatedly against an Austrian politician and former Member of Parliament. The politician demanded that the scope of a stay-down order concerning defamatory comments against her person be extended to cover equivalent comments. Following the confirmation of the validity of such an order against *Facebook* by a Higher Court in Austria, the social network appealed the ruling to the Austrian Supreme Court. *Facebook* claimed that such an order would require the network to monitor the entirety of its traffic and therefore violate Article 15 ECD, which prohibited the imposition of general monitoring obligations on intermediary service providers. The Austrian Supreme Court referred the case to the CJEU for further clarification.

The CJEU ruled in October 2019 that *Facebook* could in fact be forced to implement stay-down orders for identical comments that were made by *any* user of the social media site against the Austrian politician. Moreover, *Facebook* could be compelled to identify and prevent equivalent defamatory comments from the *same* user under the condition that any variation in the nature of the remarks did not necessitate that *Facebook* engage in a new, independent assessment. The CJEU judged that such an order was proportionate if the original injunction contained enough specific elements that allowed *Facebook* to identify the equivalent defamatory nature of the comments without engaging in an independent assessment. Such elements would be: the name of the person concerned by the infringement, the circumstances under which the infringement was determined and an indication of content equivalent to that already declared illegal. The implication by the court was that the specificity of the injunction would allow *Facebook* to deploy automated search tools. This specificity also ensured that the intermediary would not be obliged to monitor its network on a general basis for unlawful content or activity.[789] By implication, requiring the intermediary to assess anew every uploaded comment with regard to its potentially equivalent meaning would be excessive.

788 *Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 463).
789 ibid 45–47.

The decision has been viewed as backing the use of automatic filtering software and weakening the liability protections of Article 14 of the ECD.[790] On the other hand, it could also be argued that this reasoning continues the line of certain rulings in Germany, where the use of automated content recognition tools was explicitly endorsed, while a reliance on manual reviews was rejected as imposing a too high burden on the intermediary. It is, however, interesting that the CJEU appears to compare the independent assessment, read: human involvement, to the general monitoring obligation rather than judging it merely as excessive. This suggests that, rather than a direct endorsement of automated tools, the CJEU considers that automated software would lower the burden on the intermediary to effectively enforce this somewhat broader injunction. Arguably, in the absence of such technology it would be unthinkable to compel intermediaries to suppress unlawful content that contains equivalent wording. This argument appears to be in accordance with the European Commission's more recent move to support the use automated filtering systems in order to detect and prevent specific infringements.[791]

In his Opinion, the Advocate-General usefully distinguished between intermediaries' preventive efforts in the area intellectual property, such as in *L'Oréal v EBay*, and in defamation cases, like the one at hand. Given the nature of intellectual property, it was justified to restrict the mandatory preventive efforts by intermediaries in this area to new infringements of the same kind of the same rights.[792] By contrast, defamatory acts are rarely repeated in exactly the same way, by using precisely the same terms for the same type of offense. This justified a seemingly broader formulation of a preventive injunction.[793] However, applying this broader scope to all users would amount to a general monitoring obligation. The intermediary would become an active censor and loose its neutral character.[794]

---

790 Daphne Keller, 'Filtering Facebook: Why Internet Users and EU Policymakers Should Worry about the Advocate General's Opinion in Glawischnig-Piesczek' (*Inforrm's Blog*, 7 September 2019) <https://inforrm.org/2019/09/08/filtering-facebook-why-internet-users-and-eu-policymakers-should-worry-about-the-advocate-generals-opinion-in-glawischnig-piesczek-daphne-keller/> accessed 25 October 2019.

791 European Commission, 'COM (2017) 555 Final' (n 69) 14–15.

792 *Opinion of Advocate General Szpunar on Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 264) paras 68–69.

793 ibid 70.

794 ibid 73.

The broad horizontal focus of the ECD may be a problem in the context of this more differentiated case law arising out of the CJEU and Members States. As demonstrated, the reach of preventive obligations is likely to depend on the type of violations at stake and the business model of the platform operator. Balancing acts could result in different results, contingent on the type of interests involved in protecting e.g. personality rights, intellectual property rights, public security or consumer protection interests. Accordingly, the reach of proportional preventive duties could vary for hate speech, trademark violations, defamation, copyright infringements, child abuse or illegal products. Some of the larger online or social media platforms may be confronted with all of these problems at once and require differentiated responses, safeguards and technologies depending on the type of content involved. The monolithic design of the ECD seems ill-fitted to provide that level of flexibility.

3. Summary of legal challenges of the ECD

The above discussion has illustrated the complex challenges of establishing effective remedies and legal enforcement mechanisms for unlawful activity and content on online intermediaries under EU law. The specific legal framework of the ECD, set up to deal with the liabilities of mere conduits and information hosts in the intermediation of information exchanges, has been subject to serious tests. Originally set up to protect the new enablers and facilitators of communication via the internet against undue burdens and interference in the dissemination of content, it is now increasingly seen as outdated, inflexible and morally unjustified. Three paramount legal challenges have been identified that hinder an effective fight against the ongoing and diverse problem of unlawful content.

I. Summary: The availability of the ECD protections

The requirement of the "mere technical, automatic and passive" intermediary service is troubled in its application to modern-day online platforms. Indeed, this assessment is one of the most difficult to make when having to determine the availability of the liability exemptions for online platforms. The variety of platform business models, the fervency with which content is shared and the opaqueness of content dissemination and manipulation practices have made a clear-cut assessment almost impossible. However,

the decision is a key one. Under the current ECD provisions, it determines the availability of generous liability exemptions. An intermediary that qualifies as a neutral actor is subject to secondary liabilities at most. If not, however, it may face the full blow of primary liability under the relevant legal provisions that govern the content in question under national or EU law.

Meanwhile, there will likely be other, newer digital platform services, for which the application of the current hosting service definition may prove similarly difficult to judge. For example, the position of mobile web portals, cloud services, collaborative or participatory platforms or IoT platforms are just some examples.

The availability of the hosting defence has been discussed by judges, lawmakers and other specialists mainly in relation to the distinct business activities (e-commerce, content sharing, access provision), specific service features (advertising, fulfilment, comment function), technical features and content management practices (sorting, display, recommendation). These considerations would in the widest sense correspond to the complex architecture/infrastructure and design choices of platform operators.[795] Online platforms today assert almost exclusive control and power over these design choices. Most of these choices are aimed at maximising data capture, engaging multiple market actors and steering user behaviour towards more interaction and tenure on the platform.[796] The above deliberations have shown that it is by now more than doubtful that the current distinction between passive and active platforms can hold. Given how today's digital platforms govern user interaction, they have almost exclusively ceased to be "merely technical" actors in the original sense of the meaning 20 years ago.[797] Consequently, and in the absence of clear legal rules, courts in EU members continue to struggle with coming to coherent decisions in that matter. Moreover, looking for such a decision may be missing the point and hinder the formulation of effective rules that are adapted to fight unlawful content online.

It has been argued that the creation of new intermediary service provider categories in the ECD could be a way to clarify the availability of

795 Lorna Woods, 'The Duty of Care in the Online Harms White Paper' (2019) 11 Journal of Media Law 6, 13–15. Poell, Nieborg and Van Dijck (n 523).

796 Poell, Nieborg and Van Dijck (n 523). Olivier Sylvain, 'Intermediary Design Duties' (2018) 50 Connecticut Law Review 203.

797 Zuboff (n 5); Martens (n 53); Pasquale (n 19); Helberger, Pierson and Poell (n 68).

the ECD's Article 14 for new Web 2.0 platforms.[798] However, this approach risks to be overtaken by developments in the markets, possibly even before the necessary legal changes are put in place. It could also undermine the technology-neutral direction of the ECD. An alternative way could be to scrap the distinction between neutral and active intermediaries altogether. As has been shown, this assessment requires deeper technical and operational understanding of the platform models at hand. This is often not available in the courtroom nor would it be practical to enshrine more detailed criteria into the law. Why pursue this question when it has become clear that for most of today's Web 2.0 platforms, the data and content generated by user interaction, is at the heart of their business models? It generates massive profits, which even leads these actors to actively steer user behaviour. The neutrality claims of many of these intermediaries sit rather uncomfortably with the intrusive nature of their activities and the profits generated from user data. It appears that this way of thinking has found its way into the European Commission. The early version of a leaked preparatory document of the future "Digital Services Act" gives up on insisting on a distinction between active and passive hosts.[799] Unfortunately, this thinking has not prevailed in the formulation of the DSA proposal published in December 2020. As will be suggested further below, the availability of the intermediary liability exemptions should be rather tied to broader technical and design considerations of platforms.[800]

II. Summary: The knowledge standard

The assessment of actual knowledge of infringing activity and content is closely tied to the above question of neutrality. A purely neutral host under the current framework would hardly be in a position to gain knowledge of unlawful content other than by being notified of it. The US intermediary liability framework clearly follows this line in the most consequent fashion. In the EU, however, judges across Member States and the CJEU could not help but assessing the knowledge requirement in light of the increasingly immersive activities of Web 2.0 intermediaries. This was

798 European Commission, 'Synopsis Report on the Regulatory Environment for Platforms' (n 539) 16 fn 500.

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

800 See also: Sylvain (n 795); Lorna Woods and William Perrin, 'Online Harm Reduction – a Statutory Duty of Care and Regulator' (Carnegie UK Trust 2019).

certainly helped along by the fact that there are no common requirements for NTD procedures and no explicit protections for "Good Samaritans." Jurisprudence in the EU culminated in the diligent economic operator standard and the consideration of "should have known" knowledge in *L'Oréal v eBay*. Actual knowledge of unlawful activities could be gained from proactive activities or even awareness of certain facts and circumstances. Meanwhile, diverging approaches towards determining actual knowledge have persisted, again, due to the complex nature of today's intermediaries, but also due to the different national legal cultures and approaches of dealing with secondary or intermediary liability. These diverging approaches have resulted in an uneven enforcement landscape and legal uncertainty with regards to the obligations of intermediaries *vis-à-vis* unlawful content.

The question of actual knowledge of unlawful information of today's more complex and globally operating platforms touches on deeper questions of corporate epistemology[801] in a business organisation: how is information that resides in a company's infosphere, its systems, documents and people, managed? At what stage can knowledge and therefore potential liability be inferred?[802] This problem is not unique to internet intermediaries but it exists across various areas of economic life, where it is addressed through standards of corporate responsibility.[803] The question acquires a new significance when seen in conjunction with the discussion about the gatekeeping roles of internet intermediaries for information exchange in today's society.[804] Is a strict qualification of actual knowledge still appropriate or would broader concepts that incorporate constructive knowledge and corporate responsibility be more apt today?[805] The question shall be discussed in more detail in Chapter 6, where an approach towards a new responsibility framework will be explored.

801 Burk (n 295) 451–453.
802 Burk (n 296), who borrows his approach from Floridi's concept of information ethics and the concept of infosphere: Luciano Floridi, 'Information Ethics: On the Philosophical Foundation of Computer Ethics' (1999) 1 Ethics and Information Technology 33.
803 Burk (n 295); Helberger, Pierson and Poell (n 68).
804 Taddeo and Floridi (n 120).
805 Valcke, Kuczerawy and Ombelet (n 551) 113.

III. Summary: Specific versus general monitoring

Finally, establishing when a specific monitoring or prevention obligation becomes a general one has been another tricky point. It took Member States considerable time to acknowledge more generally that stay-down orders did not result in general monitoring obligations. Meanwhile, the reappearance of once notified content throughout the internet remains a problem. This is also helped along by the nature of the internet and digital information exchange as a succession of copying instances. The ongoing wide availability of unlawful content has led to calls by legislators and enforcers for enlisting online intermediaries more proactively in this battle. Soon the attempt to ask intermediaries to prevent unlawful information beyond the suppression of already notified material hit the wall of Article 15 ECD. This provision was originally set up to protect the new intermediary sector against undue burdens of manually reviewing information that they transmitted or stored, and to shield them against attempts to use them as censors. However, with their rise in importance and with improved filtering and surveillance technologies, pressure mounted on intermediaries to broaden their preventive monitoring.

The ECD did not provide enough clarity in this respect. Courts have struggled to find the dividing line between general and specific monitoring. They developed different approaches, which, predictively, led to differing interpretation on the permitted proactive obligations of online intermediaries. It appears that the terms of specific and general monitoring are moving targets, driven mainly by technological change. Proactive measures that 15 years ago would have necessitated significant manual correction and *de-facto* general monitoring may today be less intrusive, more targeted and effective.[806] Thanks to advances in content recognition, data inspection and analytics they could today be seen as "specific", reasonable and proportional.[807]

The CJEU attempted to define the scope of more proactive, but specific monitoring obligations (*L'Oréal v eBay*, *Facebook*) and distinguish them from excessively broad monitoring duties (*Scarlet Extended*, *Netlog*). However, it appears that the CJEU relied in its fundamental rights balancing exercises on the safeguards provided for in the sectoral legal provisions specific to the content involved. In that sense, Article 15 ECD may have in-

806 Woods, 'The Carnegie Statutory Duty of Care and Fundamental Freedoms' (n 698) 11; Edwards and Veale (n 698) 82–83.

807 Friedmann (n 16) 152–153.

deed become an empty shell.[808] Preventive obligations change in proportion with technological progress and the type of violation and harms involved. The scope of permitted monitoring should not be limited by a diffuse concept of "generality" but rather be determined by proportionality that is derived from balancing the unlawful acts with the specific fundamental rights involved. The futile quest over the dividing line between general and specific monitoring duties of intermediaries has impeded the more important task of defining proportional and effective proactive obligations for online intermediaries in the fight against unlawful content.

808 Sophie Stalla-Bourdillon, 'Internet Intermediaries As Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well.' in Mariarosaria Taddeo and Luciano Floridi, *The responsibilities of online service providers* (Springer Berlin Heidelberg 2016) 287 .