Chapter 6 - A new framework for online intermediary responsibility

This work has so far outlined various problems with unlawful content propagated through online intermediaries. Chapter 2 sketched the stellar rise and evolution of online platforms as essential facilitators of information exchanges and gatekeepers to the internet over the last two decades. Chapter 3 provided the backdrop of a broad horizontal legal framework of liability exemptions that has been resting on essentially unchanged premises for 20 years. It demonstrated that three main liability conditions – neutrality, actual knowledge and the scope of (preventive) obligations – are outdated and would need to be replaced by new criteria that allocate responsibilities that are in line with the commercial and technical involvement of platforms in the intermediation process. Chapter 4 outlined the specific problems of the interaction between the outdated horizontal liability framework and content specific laws both in national and EU contexts. The avenues explored in response to unlawful information shared through online platforms ranged from primary liability, enhanced secondary liabilities based on duty of care obligations, the formulation of new offenses specific to information intermediaries to the use of ordinary law secondary liability doctrines. The regulatory choices included various self-regulatory arrangements, solutions that went into the direction of co-regulation and more straightforward rule and command style interventions. All this has been accompanied by ample jurisprudence, which partly served as a blueprint for the new regulatory advances.

Academics, industry representatives and think tanks have not been standing by idly. Various intermediary liability (exemption) reform proposals have seen the light since 2007. The frequency with which these proposals appeared has increased markedly over the last five years. Some focus on specific violations, others on particular types of platforms. Yet others are more occupied by the type of regulatory intervention or the specific liability standard. Almost all grapple with the question of how enhanced public interest responsibilities can be implemented in a way that protects the precarious balance of fundamental rights that will inevitably be affected when regulating information gatekeepers' content management practices.

In the following, a number of reform approaches and proposals will be outlined and evaluated. This overview will serve as a basis for a more theoretical discussion. It will first be used to critically assess the regulatory choices of a new intermediary responsibility framework. The particular characteristics of the internet, its intermediaries and the broad nature of unlawful activity and content call for a carefully gauged level of regulatory intervention. Secondly, the discussion will move to the type of responsibility that would be more adequate given the developments and challenges discussed throughout this work. For example, can a primary liability approach be reconciled with certain types of intermediary responsibility, such as duty of care? Lastly, a reform proposal will be put forward that advocates for a move away from liability towards a broader responsibility framework. The suggested solution will also advocate for closer state involvement in the form of co-regulation. This would allow for better oversight and enforcement of the adherence to public interests and fundamental rights that are affected by online platforms' content management practices.

A. Intermediary responsibility reform proposals – an overview

The overview of intermediary liability reform proposals discussed below does not claim to be exhaustive. The proposals were selected according to their comprehensiveness and to the degree to which they inspired the approach suggested later in this chapter, either because of corresponding assessments or by providing conceptual demarcations. Many of the proposals analysed below advocate for enhanced responsibilities of online platforms through obliging them to apply duties of care that are proportional to their involvement in the intermediation process. This commonly results in online intermediaries needing to a) be aware of and evaluate the possible harms and ensuing risks of their business model with regards to unlawful content or activity, b) design and implement measures to address these risks *ex ante* and *ex post*, c) ensure the risk responses are transparent and accountable and comply with legal standards.

1. Systemic approaches

As early as 2007, less than 10 years after the enactment of the ECD, *Verbiest et al* saw a need for an overhaul of the intermediary liability system.[1688] They started from the observation that the ECD did not create any incentives for intermediaries to prevent future similar infringements of those notified to them. However, they rejected a negligence-based approach that would task courts with developing such standards. Already at the time, courts across the EU diverged in their interpretation of liability (exemption) standards towards intermediaries. The fear was that asking courts to create negligence standards would result in widely different outcomes. Secondly, waiting for court-made law would simply take too long. In addition, this depended on relevant cases being brought before judges. Instead, *Verbiest et al* looked to the example of the *New Approach*, used in product safety regulation.[1689] EU legislators would ask European standardisation committees (CEN) to develop technical standards of filtering that would apply to specific content sectors. Intermediaries, rightsholders and other stakeholders would take part in such a standard creation. The standard could be adapted to evolving technologies and would be considered by courts in their assessments. In content sectors where such standards existed, providers could be ordered to use them in order to stop repeat infringements. Like under the *New Approach*, the adoption of these standards would be voluntary. ISPs could deploy their own solutions, but would need to demonstrate that these are equivalent to the relevant technical standard. Finally, failure to comply with such a standard would result in comprehensive filtering obligations. Non-profit ISPs would be exempt.[1690]

Helman and Parchomovsky (2011) pursued a similar idea for copyright infringements by proposing a "best available technology safe harbour." This standard would replace the current DMCA liability provisions and exempt online intermediaries from liability where they had used the best available technology to prevent infringements.[1691] Government agencies would determine which technologies and solutions were considered as best filtering technology. Their proposal is motivated by the fact the US intermediary

1688 Verbiest and others (n 315) 20–23.
1689 ibid 22.
1690 This proposal was repeated in 2016: Gerald Spindler and Christian Thorun, 'Die Rolle Der Ko-Regulierung in Der Informationsgesellschaft' (2016) 6 MMR-Beil. 1, 24.
1691 Helman and Parchomovsky (n 309).

framework of the DMCA disincentivised information hosts to filter and monitor for infringing content, except for very narrowly construed "red flag" content. They use cheapest cost avoider, economic reasoning for tasking online intermediaries with stronger obligations to participate in the prevention of copyright infringements.[1692] Not only are online intermediaries technically and infrastructurally best placed to monitor, prevent and remove infringing content. Their activity would also alleviate the need for content owners to engage in duplicate efforts.[1693] *Helman and Parchomovsky* advocate for collaboration between intermediaries, content owners and technology providers in the operation of prevention technology. While webhosts would perform the filtering, their analysis would be based on technology developed by copyright clearinghouses, which would rely on one central, government-held copyright database. They note that independent clearinghouses would have the highest incentive to strive for accurate technology, e.g. with regard to determining fair use exceptions.[1694] In contrast to *Verbiest et al*, this approach does not just apply to the prevention of repeat infringements, but to any copyright infringements, as deemed fit by the best technology standards.

Busch (2018) has adopted the use of *New Approach* technical standards to online reputation systems. Although the focus of his work is not on unlawful content, the proposal suggests the application of such a co-regulatory system to the entire 'platform ecosystem'.[1695] Technical standardisation may be more apt than traditional command and control regulation on the one hand, and codes of conduct on the other, to provide flexibility in the fast-changing and highly technical setting of the internet, while at the same time providing procedural transparency.[1696] In addition, the technical standards approach fits within the EU's strategy to expand the use of technical standards as a soft law instruments and apply it notably in the

1692 ibid 1202, 1212.
1693 ibid 1203.
1694 ibid 1215–1223.
1695 Christoph Busch 'Towards a "New Approach" for the Platform Ecosystem: A European Standard for Fairness in Platform-to-Business Relations' 3.
1696 Research Group on the Law of Digital Services, 'Discussion Draft of a Directive on Online Intermediary Platforms' [2016] Journal of European Consumer and Market Law 164, 165; Christoph Busch, 'Crowdsourcing Consumer Confidence - How to Regulate Online Rating And Review Systems in the Collaborative Economy' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution* (Intersentia 2016) 231–232.

area of information and communication technologies (ICT).[1697] The eventual solution showcased by *Busch* refers to an ISO standard for online consumer reviews.[1698] A European Commission study by *van Eecke* (2009) proposed the creation of sector specific technical standards for the interaction between rightsowners and online platforms in the identification of infringing material. This concept could also be applied to NTD mechanisms, including counterclaims procedures.[1699]

Kempel and Wege (2010) explore the establishment of a risk management system that would help internet intermediaries determine reasonable duties of care that were starting to be formulated in intermediary liability jurisprudence at the time. They note that courts had come to different interpretations of what could be considered reasonable efforts for ISPs.[1700] This created legal uncertainty for ISPs and imposed incalculable liability risks. Any risk mitigation through excessive content monitoring could lead to the ISP gaining actual knowledge, while no or insufficient control could lead to courts finding the ISP had neglected its duties of care. They suggest that ISPs use a risk management methodology to adequately identify, analyse, evaluate and control risks related to unlawful content on their systems. Regulations, they argue are not suited to provide detailed and pragmatic risk management duties. By contrast, technical norms or standards are suitable instruments for defining adequate duties of care based on a risk management approach. Technical norms under the European standardisation approach are capable of defining state of the art requirements while establishing proportionality (reasonableness), due to their stakeholder approach.[1701] Once defined, these technical standards can be referenced as a legally binding standard in legislation. The ECD's Recitals 40 and 41 underline the intention of the EU to promote the creation of such standards. This proposal mirrors suggestions by *Verbiest et al* who made use of *New Approach* style regulation. For *Kempel and Wege* technical norms have the

1697 European Commission, 'Communication: ICT Standardisation Priorities for the Digital Single Market COM(2016) 176 Final' <https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market> accessed 29 August 2018.

1698 Technical Committee : ISO/TC 290 Online reputation, 'ISO 20488:2018 - Online Consumer Reviews — Principles and Requirements for Their Collection, Moderation and Publication' <https://www.iso.org/standard/68193.html> accessed 21 July 2020.

1699 Van Eecke and Truyens (n 316) 42.

1700 Kempel and Wege (n 16) 107–108.

1701 ibid 116–118.

advantage of being adaptable to the fast technological development of the internet. They are international and respond to the cooperative character of internet content by allowing for an allocation of responsibilities to different stakeholders.[1702] By contrast, they may not be of particular use for adapting to different business models or for defining prospective responsibilities, they argue. The latter is based on the fact that their proposed system is mainly looking at the management of the risk of unlawful content and therefore existing user behaviour. The degree to which a platform operator may profit, intentionally or unintentionally, from the unlawful behaviour of third parties would best be established by law.[1703] However, later proposals by e.g. *Woods and Perrin* or *Helberger*, described below, argue that co- or self-regulatory systems may well be capable of incorporating prospective responsibility criteria, such as "by-design" concepts into responsibility frameworks.

One of the most detailed and comprehensive proposals for a statutory duty of care for online platforms has been made by *Woods and Perrin* (2018).[1704] This proposal has been adopted by the UK Government's White Paper to deal with the harms caused by unlawful and harmful content on social media.[1705] *Woods and Perrin* see social media platforms as quasi-public spaces on which significant parts of the population convene, communicate or look for goods and services to buy. This 'utility' approach to modern day online intermediaries has also been supported by others, such as *Pasquale, Wagner* or *Helberger.*[1706] This quasi-public character of online platforms entails certain duties of care to protect the public against harms that could be caused by the use of these digital spaces. They point to equivalent legal obligations in more traditional areas:[1707] employers need to protect their workers against damage to health and safety; under environmental protection regulations entities handling, producing or disposing of waste have particular duties that depend on the type of activity and the

1702 See also Herberger et al' s concept of cooperative responsibility: Helberger, Pierson and Poell (n 68).
1703 Kempel and Wege (n 16) 120.
1704 William Perrin and Lorna Woods, 'Reducing Harm in Social Media through a Duty of Care' (*Carnegie UK Trust*, 8 May 2018); Lorna Woods, 'Duty of Care' (2018) 46 InterMEDIA. Woods and Perrin (n 799).
1705 Great Britain and Department for Culture (n 197).
1706 Pasquale (n 19) 297–300; Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' (n 83) 235–236; Helberger (n 1651) 167.
1707 Woods and Perrin (n 799) 21–28.

type of waste involved; the GDPR makes entities that collect and process personal data accountable to do this according to specific principles. Under the GDPR, data controllers need to secure and protect personal data according to the level of risk.[1708] Entities with high risk personal data processing activities need to perform impact assessments. The common theme is, that companies are tasked with duties to assess the risk of harms facilitated or caused by their business activity and put appropriate measures in place to address them.

Focussing on social media platforms, *Woods and Perrin* define harms which may arise from content and intermediation practices and which trigger the public interest. These harms correspond broadly to the sectors touched on in Chapter 4. Economic harms include copyright and trademark violations; terrorist speech would fall under national security harms; hate speech and defamation would fall under harmful threats, emotional harms or harms to minors.[1709] Social media service operators would then be tasked to assess the risk of each harm in the context of their business model and architecture. They would need to devise and implement measures to address and prevent the most significant harms and risk. The regulator would provide guidance on the risk assessment approach for social media service operators and assess the outcomes of the measures taken by platforms. *Woods and Perrin* propose that successful common approaches to harm reduction and risk management be set out by industry codes of practice, which are endorsed by regulators. This would allow for flexibility and customisation given the fast pace of innovation in this sector.[1710] These codes would also allow for the establishment of forward looking or prospective responsibility criteria such as safety-by-design.[1711] The regulator would also set out basic procedural and "structural requirements" for regulated platforms. Platforms would need to provide proof of their risk assessment procedures (for example risk rating and new service review mechanisms), parental control systems, complaints handling procedures or any other broad requirements established by the law. Under this co-regulatory structure, the regulator would have a set of broad guidance and approval functions such as publishing transparency reports, guidance notes,

1708 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data 2017 (OJ L 119, 452016) Articles 5, 25, 32 (1), 35.
1709 Woods and Perrin (n 799) 35–42.
1710 ibid 46.
1711 ibid 47.

model policies, approve codes of practice and facilitate society stakeholder dialogue and research.[1712] In that sense, this proposal is not dissimilar from the role attributed to the *CSA)* under the recently failed *Loi Avia* in France. *Woods and Perrin* do not foresee, however, specific exemptions for smaller players.[1713] They also apply their principles in an overarching way for each platform at 'system level', and would not create different regimes for different content sectors or types of activities.[1714] However, it remains unclear how current sectoral provisions, some of which have now extended primary liability towards online platforms, i.e. in copyright, could be (re)integrated into this framework. It appears obvious from the iterations of *Woods and Perrin* that they propose to create a specific responsibility regime for platforms, thus excluding the allocation of primary liabilities under substantive law, such as copyright or defamation.

Valcke et al. (2017) have also argued for the necessity of a new duty-of-care standard that online platforms adopt in order to remove and prevent unlawful activity and content. They base their approach on the diligent economic operator standard, first formulated in the CJEU case *L'Oréal v eBay*, and subsequently refined in *GSMedia*, *UPC Telekabel* and *Delfi (ECtHR)*. They liken these responsibilities to the Roman law doctrine of *bonus pater familias*. Industry self-regulatory codes of ethics or conduct, such as those drawn up by national press or journalism councils, could serve as a blueprint for similar standards and principles for internet intermediaries. Under these codes, behaviour would be seen as unethical or irresponsible where a platform failed to take steps that could be reasonably expected of it under such codes in order to prevent unlawful content or behaviour. In *Delfi's* case this was the failure to take sufficient account of the risk that the comments function it provided could be abused for hate speech. Courts could use these standards as a yardstick when confronted with liability disputes over unlawful content.[1715] In a similar vein, *Leistner* (2014) suggests a broad analysis of EU national case law on intermediary liability.[1716] The focus would be on an evaluation of cases where preventive measures were imposed on ISPs. The idea is to extract new common principles that would be developed into an EU wide reasonable duty of care standard. The proposal focusses on the area of IP infringements. However, he rejects the use

1712 ibid 48–49.
1713 ibid 35.
1714 ibid 12.
1715 Valcke, Kuczerawy and Ombelet (n 551).
1716 Leistner (n 336) 89.

of self-regulatory industry standards, as proposed by *Valcke et al.* Such standards, if developed by present market actors (large intermediaries and rightsowners), bear the risk of being biased towards their interests, to the detriment of less economically powerful users.[1717]

The concept of reasonableness has also been exploited by *Waisman et al* (2011), who propose a flexible standard of duty of care for search engines.[1718] Like *Leistner* and *Valcke et al*, they trace the evolving duty of care concept through European case law and suggest the allocation of flexible, reasonable duties. The degree of reasonable care would follow the consideration of certain criteria, such as the scope, cost, harm and impact on fundamental rights of any duties of care applied to search engines. Reasonableness with regards to the costs of a duty of care would, for example, take into account whether this prevents the provision of socially valuable services or poses a market entry barrier. A further threshold of reasonableness would be the undue restriction of freedom of expression.[1719]

Finally, *Lavi* (2015) explores a context-based liability regime for social media and UGC platforms.[1720] Focussing on speech acts under the CDA in the US, he starts form the by now familiar argument that the active/passive dichotomy and the far-reaching liability immunities facilitate the development of technology that promotes behaviour that society normally prohibits. In addition, it discourages intermediaries from designing safer systems.[1721] *Lavi* advocates for a scaled liability system that imposes gradually increasing penalties allocated under inducement liability at the beginning of the spectrum, to contributory liabilities at the extreme side.[1722] The severity of the liability and the ensuing penalties would depend on the strength of intent, actual knowledge and the effect of the platform's nudges, i.e. the way in which architectural and design choices promote unlawful and harmful user behaviour.[1723] Courts would allocate these penalties. This would serve as a deterrent for online platforms to engage in biased and opaque nudging practices. *Lavi* sees the reliance on transparency obligations for intermediaries that engage in biased nudging practices as

1717 ibid.
1718 Waisman and Hevia (n 313).
1719 ibid 799–802.
1720 Michal Lavi, 'Content Providers' Secondary Liability: A Social Network Perspective' (2015) 26 Fordham Intell. Prop. Media & Ent. LJ 855, 888.
1721 Lavi (n 199) 62.
1722 ibid 82–84.
1723 ibid 79–82.

problematic, because of many users' proven disinterest and incomprehension of disclosure statements.[1724]

2. Procedural approaches

A number of researchers focus on the application of due process requirements on online intermediaries. *Wielsch* (2019) argues that it would be reasonable to charge online intermediaries with the protection of fundamental rights through procedure. He justifies this with the quasi role of online intermediaries as speech regulators.[1725] This is part of a wider societal trend to charge multinational corporations with the protection of fundamental rights, at least where it concerns communication infrastructure providers. The CJEU had already confirmed this in *UPC Telekabel*.[1726] Duties of care would constitutionalise internal standards of speech regulation when it comes to unlawful content, leading to the development of 'public standards of legality'.[1727] The German *NetzDG* is a case in point of institutionalising these procedural requirements. In the *NetzDG*, failure to delete unlawful content is not a punishable act, while failure to have effective and transparent complaints handling systems in place is.[1728] *Gillespie* (2018) suggests that online platforms be obliged to follow public standards on how content is moderated, rather than standards on what content to remove.[1729] These public standards could be formulated through: transparency reporting obligations; minimum moderation standards, such as response times or appeals processes; data sharing practices with researchers; the involvement of external expert advisory panels; labour protection standards for moderators; data portability obligations.[1730] This view is supported by *Laidlaw*, who calls for a codification of rules on how platforms moderate content based on due process principles.[1731] *Bambauer* (2018) de-

1724 ibid 90.
1725 Dan Wielsch, 'Private Law Regulation of Digital Intermediaries' [2019] SSRN Electronic Journal 14–20 <https://www.ssrn.com/abstract=3369592> accessed 3 May 2019.
1726 *Telekabel* (n 757) para 55. In: Wielsch (n 1724) 17.
1727 Wielsch (n 1724) 17.
1728 ibid 19.
1729 Gillespie, 'Platforms Are Not Intermediaries' (n 175) 213; Gillespie, *Custodians of the Internet* (n 1010) 44.
1730 Gillespie, 'Platforms Are Not Intermediaries' (n 175) 213–216.
1731 Laidlaw (n 494) 23–24.

mands that online platforms be brought to shed light on the internal processes and mechanisms that lead to the decisions on which content removal, amplification or restoration are based.[1732] This goes somewhat deeper than the previous proposals because it requires platforms to disclose their normative choices in content moderation. This, in turn, would allow for adjustments where public interest and fundamental rights criteria are not sufficiently met. He points to the fact that most online platforms do document their (internal) content moderation guidelines and should therefore be able to explain the rationale of their decision-making when moderating content.[1733]

Helberger et al (2018) focus on the governance mechanisms of online platforms. Traditional legal systems tend to allocate main responsibility and liability to a single actor. The active/passive dichotomy of information hosts under the ECD is a case in point.[1734] In reality, however, content creation and moderation on today's platforms is a more participatory exercise that relies on three groups of actors. Online platforms 'manage' user activity in this process. Users, on the other hand, can only act responsibly if the platform architecture is shaped in a way that is conducive to this, such as, for example, by providing training and education, reporting and flagging tools, or clear policies.[1735] This means online platforms are in a position to take prospective responsibilities to design their systems in a way that allows for responsible interaction of users.[1736] Regulators, the third type of actors, should be responsible for providing adequate frameworks for risk and responsibility sharing, by promoting public debates on the balancing of public values in content management. None of the three actors alone, it is argued, should bear the brunt of responsibility. *Helberger et al* propose four steps for building such a cooperative responsibility framework: First, the public values of the various intermediation activities should be defined. Secondly, responsibilities should be attributed to each actor in the protection of the public values of each sector, type of intermediary etc. Thirdly, stakeholders should agree on how they can fulfil their responsibilities. Fourthly, this should result in more formal codifications, either through regulations, codes of conduct or best practices.[1737] This frame-

1732 Bambauer (n 297) 421–423.
1733 ibid 422–423.
1734 Helberger, Pierson and Poell (n 68) 2.
1735 ibid 5.
1736 ibid 2–4.
1737 ibid 10.

work provides a useful conceptual and moral approach to allocating responsibilities and positive obligations on users, platforms and public actors. However, it leaves open the question of the regulatory choice of the risk management framework.

3. Common and divisive features of current intermediary liability reform proposals

Most of the proposals presented here have a number of things in common. First, they eschew the traditional distinction between active and neutral hosts. There is an increasingly broad consensus, that at least as information hosts are concerned, it is a futile exercise to tie liability, or the availability of immunities, to the allegedly neutral status of an online platform.[1738] Even more, none of today's Web 2.0 online platforms are absolutely neutral, because the business models rely on the exploitation of content and user behaviour, and they design their technical architectures accordingly. Secondly, the participatory nature of online platforms in the intermediation process justifies enhanced, but at the same time, nuanced responsibilities that are proportionate to the riskiness of a platform's ecosystem. Thirdly, there is an acknowledgement that today's Web 2.0 platforms significantly influence user behaviour and control access to information and commercial transactions. As quasi-public utilities they now affect the public interest in many ways, of which the harms caused by unlawful content are just one, yet high profile, aspect.[1739] Fourth, the proposed regulatory tools focus on duties of care, risk management approaches and procedural obligations (due process, transparency, fairness).

Yet, the approaches for regulating online intermediaries' liability conditions or responsibilities discussed here also vary in important aspects. For one, there are different views about the regulatory model that such a new intermediary responsibility framework should follow. While almost none of the commentators advocate for traditional command and control regulation, differences about the depth of public intervention remain. Systemic

1738 Lavi (n 199) 14; Chander and Krishnamurthy (n 883); Zuboff (n 5) l 2042; Martens (n 53) 33–35; Helberger, Pierson and Poell (n 68) 2; Sylvain (n 795) 59.

1739 Competition, data protection or consumer protection are other public interest areas where EU and national legislators have been intervening or have considered legislative action.

approaches of *Verbiest et al*, *Kempel and Wege*, *Helman and Parchomovsky*, or *Woods and Perrin*, which advocate for more defined risk management frameworks, appear to favour more or less co-regulatory solutions. The broad parameters of public interest criteria would be set through regulation. Industry is then commissioned to devise tools, mechanisms and methodologies to comply with these criteria. Regulators would have more closely defined oversight and sanctioning powers with regards to compliance with the values and principles set down by law.[1740] The co-regulatory approaches show different shades of state involvement. While *Verbiest et al* and *Kempel and Wege* favour the use of technical standards as a co-regulatory tool, *Woods and Perrin* look at codes of conduct and industry practices in order to implement regulatory provisions. They see the latter as more suited because of their flexibility and adaptability to specific risks, business models and technological change than standards.[1741] Proponents of procedural approaches that look more to jurisprudence as an inspiration of new duties of care are more divided. While some favour self-regulatory approaches (*Valcke et al*), others have voiced no pronounced view. Overall, a preference for self-regulatory solutions is, however, visible.

It should also be said that the approaches discussed here vary widely in scope. While some propose overarching frameworks and methodologies (*Woods and Perrin*, *Helberger*), others focus on specific types of platforms or contents (*Lavi*, *Waisman et al*), specific processes, like content moderation (*Bambauer, Laidlaw, Gillespie*) or consider retrospective responsibility aspects such as duties of care for prevention, detection and removal of unlawful content (*Verbiest et al, Kempel and Wege, Helman and Parchomovsky)*. Proposals that concentrate on retrospective responsibilities belong to earlier reform attempts. The inclusion of prospective, "by-design" responsibilities has only happened more recently, after 2015.

For completeness, it should be mentioned that there are also commentators that see less of a need to change the current intermediary framework.[1742] Some point out that the trend towards "responsibilisation" of intermediaries might lead to more opaque private speech regulation on the

1740 For a more detailed definition of co- and self-regulation see the next section.

1741 Woods and Perrin (n 799) 27.

1742 Savin (n 384) 173; 'Open Letter on Intermediary Liability Protections in the Digital Single Market' (*EDRi*, 28 April 2015) <https://edri.org/open-letter-on-intermediary-liability-protections-in-the-digital-single-market/> accessed 28 October 2019. Savin (n 482).

Internet.[1743] However, it should be underlined that it is the aim of a functional and adequate new responsibility framework to improve due process, accountability and transparency standards. If left as is, online platforms will continue in opaque content moderation practices that follow entirely commercial objectives, without facing significant liabilities for the harm to public interests and fundamental rights caused.

B. The regulatory choice of a new intermediary responsibility system

1. The current regulatory choice

The diversity of regulatory approaches towards new platform responsibilities is also reflected in the regulatory initiatives put forward at EU and Member State level. The European Commission's facilitation of industry-driven, voluntary codes of conduct and memoranda of understanding[1744] betrays its initial penchant for self-regulatory arrangements. This style of regulatory interventions is explicitly supported by the ECD.[1745] The EU saw self-regulation as a more flexible tool than Directives or Regulations[1746] to deal effectively with the rapid market and technological changes introduced by the internet. But even with its latest legislations, such as the DSMD, the EU does not seem to have departed from its self-regulatory path. The best efforts of OCSSP to prevent copyright infringing content in the absence of any licensing agreements, will be judged, amongst others, on the use of high industry standards of professional diligence.[1747] However, the definition of such standards is merely facilitated by the European Commission and Member States, who are supposed to bring together industry and user stakeholders to exchange best

1743 Belli and Sappa (n 42) 183; Giancarlo Frosio F, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' [2017] Northwestern University Law Review Online 20.

1744 See the initiatives at EU and national level mentioned in Chapter 4: 'Code of Conduct on Countering Illegal Hate Speech Online' (n 542); European Commission, 'EU Internet Forum' (n 1061); European Commission, 'Memorandum of Understanding on Online Advertising and Intellectual Property Rights' (n 542); 'Memorandum of Understanding on the Online Sale of Counterfeit Goods, 2016' (n 542); Bundesministeriums der Justiz und für Verbraucherschutz (n 953).

1745 Directive 2000/31 (ECD) Article 16.

1746 Lodder and Murray (n 448) 54.

1747 DSM Directive 2019/790 Article 17 (4) (d), Recital 66.

practices.[1748] Public authorities or regulators do not appear to have any more formal role in the approval or audit of best efforts.

The AVMSD, by contrast ventures more into co-regulation by tasking ERGA with coordinating and providing technical advice in regulatory matters in the area of hate speech. Admittedly, merely providing advice may be considered as not sufficient to count as proper co-regulation. On the other hand, the mere existence of a formal regulatory body that has been appointed with a defined role and tasks, although these are more informal in nature, can be considered as a first step away from self-regulation into the area of co-regulation.[1749] The now failed *Loi Avia* is similar in that respect. It established an overarching regulatory agency, the *CSA*, with defined powers of overseeing ISPs' efforts in the fight against hate speech and other unlawful content. The TERREG proposal goes even further. Like the DSMD and the AVMSD, it asks hosting providers to put specific preventive measures in place that are commensurate to the risk of unlawful activity. However, providers subject to a high risk of terrorist content sharing will need to report on their specific preventive measures to competent public authorities. Authorities have then the power to evaluate the measures taken by the platforms with regards to their proportionality and effectiveness. That assessment should consider the general risk level, the size of the platform and its resources, as well as the safeguards in place for the respect of fundamental rights.[1750]

As this work attempts to propose its own regulatory proposal to intermediary responsibility, a brief excursion into different regulatory models that are employed in the EU, and in internet regulation in general, will be discussed. The concepts of co- and self-regulation shall be elaborated on in more detail.

1748 ibid Recital 71.

1749 Taking Marsden's *Beaufort* scale of self- and co-regulation as a yardstick this could be considered a first step in the realm of co-regulation, i.e. probably Step 7. Marsden, *Internet Co-Regulation* (n 275) 227.

1750 European Commission Proposal for a Regulation to prevent terrorist content online, EP resolution (n 1122) Articles 4 , 5, Recitals 16 & 17.

2. Regulatory approaches for the internet

Wu, *Castells* and others[1751] have convincingly argued that today's connected information society is just the latest culmination of a consistent trend of industrialisation, globalisation and successive revolutions in information and communication technologies. The rise of new regulatory models that straddle the border between private and state actors is intricately linked with this trend. The theoretical explanation for this phenomenon was first provided by *Durkheim*. Living around the turn of the 20th century, *Durkheim* observed the profound social and economic changes caused by the second industrial revolution. Mass-production, urbanisation, internationalisation and technological innovation led to an upheaval in social relations and economic organisation.[1752] Modern society became more complex and removed from traditional, more communal and religious values. As traditional moral values were uprooted, they left a void, which Durkheim called *anomie*.[1753] Durkheim found that new societal relations were characterised by a specialisation and the division of labour, not just in the economic sphere but also in politics, administration and the legal system.[1754] This new division of labour, which resulted in more dense and complex interrelations within society, would eventually generate new values and rules, and displace the state of *anomie*. For *Durkheim*, the nation state was less apt to regulate complex economic and social relations and interactions of individuals in this new society. This would be done through private professional associations and through corporations. Public law would become more and more broad, stipulating mainly what was to be done, but not how it was to be achieved. Meanwhile, contracts would become more important in everyday life. In effect, the division between private and public law had already become increasingly blurred by this division of labour in *Durkheim's* time.[1755]

1751 Castells (n 3); Wu, *The Master Switch* (n 1). Naughton (n 6) 390–392. Chris Marsden, 'Prosumer Law and Network Platform Regulation: The Long View towards Creating Offdata' (2018) 2 Georgetown Law Technology Review 376, 379–381. Vincenzo Zeno-Zencovich and Giorgio Giannone Codiglione, 'Ten legal perspectives on the "big data revolution"' in Fabiana Di Porto (ed), *Big data e concorrenza* (A Giuffrè editore 2016) 30.

1752 Anthony Giddens and Philip W Sutton, *Sociology* (6. ed, Polity Press 2009) 13–15.

1753 Durkheim (n 31) ll 7043–7072.

1754 ibid 697.

1755 ibid 1182.

Durkheim's theory has influenced a variety of contemporary approaches and critiques of governance and regulation. *Schepel* sees him as a precursor to governance, deregulation and privatisation, as he explains the state's shift of specialist regulatory tasks towards the private sector, while itself assuming broader, coordinative roles.[1756] Meanwhile, *Zuboff*, picks up on *Durkheim's* warnings that certain types of unchecked division of labour may lead to inequalities and injustices in society. She compares this to predatory practices of online platforms, which perpetuate divisions of learning by producing inequalities in the way people are able to access and evaluate information and knowledge in the information society.[1757] Indeed, *Durkheim* himself saw the necessity of government or the state to oversee the respect of basic principles and norms of social solidarity and justice in order to ensure social coherence in a specialised and changing society.[1758]

Blommaert points to the breath-taking development of new social media platforms and the *Durkheimian anomies* they present for interaction between users.[1759] Users are filling these gaps with ad hoc rules and new norms rapidly. However, it is unclear how much users' actions are down to deliberate, individual choice and how much happens through the agency of algorithms managed by social media platforms.[1760] In that respect social media platforms exercise new forms of power. With their algorithms and big data analytics, they shape communities and digital user identities.[1761] The new social norms on the internet may therefore be steered and manipulated by those globally operating companies for their own purposes, which creates new inequalities. Competing norm-setting organisations, such as multinational enterprises, international organisations, globally operating professional and civil society organisations and technical standards bodies have led to a world of legal pluralism, according to *Teubner*.[1762] Public governance is made difficult, because the global internet's social processes operate at a transnational stage, while governments regulate social processes at a state level. In addition, the inertia that characterises governments and bureaucracies, often makes their regulatory actions appear

1756 Schepel (n 34).
1757 Zuboff (n 5) ll 3400–3438.
1758 Durkheim (n 31) 6220–6509.
1759 Blommaert (n 63) ll 463–478.
1760 ibid 911–924.
1761 ibid 1438, 1547.
1762 Gunther Teubner, 'Global Bukowina: Legal Pluralism in the World-Society', *Global Law Without a State* (1997).

anachronistic.[1763] The difficulties of courts and governments to adapt to the international nature of unlawful content on the internet, and the speed with which these challenges manifest themselves, have been demonstrated in the previous chapters. These anachronisms determine also the regulatory choice of measures taken to combat unlawful content online.

The following, non-hierarchical account outlines some of the main regulatory approaches and concepts that have been applied to the internet. They all represent more general attempts to tackle the legal challenges in a diversifying and increasingly complex, international economic and social order of which the internet and its information intermediaries are just one vivid expression. Given the nature of the challenges outlined beforehand, it is suggested that a new intermediary responsibility framework should adopt these policy approaches and tools.

I. Self and co-regulation on the internet

Various definitions of self-regulation exist. For the purposes here, the definition in the EU's 2003 Interinstitutional Agreement on Better Law-making[1764] shall be used as a reference. This agreement was a follow-up to the European Governance White Paper, in which the European Commission vowed to improve trust in and support for the EU project through more accountable, participative and flexible policy-making. Self- and co-regulation were identified as new approaches that would help to achieve more effective, simpler and faster regulation.[1765] According to the 2003 Interinstitutional Agreement on Better Law-making self-regulation is defined as:

> "*…the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements).*"[1766]

The definition at hand is useful because it provides a clear demarcation line to co-regulation. Some commentators have classed co-regulation as a

1763 Blommaert (n 63) ll 708, 1406.
1764 Interinstitutional agreement on better law-making, OJ C 321/01 2003.
1765 European Commission, 'European Governance - A White Paper, COM(2001) 428 Final' (European Commission 2001) 18–21. See also: Senden and others (n 1654) 5.
1766 Interinstitutional agreement on better law-making, OJ C 321/01 para 22.

self-regulatory approach,[1767] while for others the dividing line seems to be less clear or relevant.[1768] For *Senden*, the determination of co-regulation versus self-regulation depends on the state, nature and intensity of public involvement in the policy cycle.[1769] A majority of experts, however, draw a methodological and conceptual line between co- and self-regulation, especially where it concerns more complex areas of technology regulation.[1770] For *Marsden*, co-regulation consists of a complex interaction of general (state) legislation and self-regulation, which gives a sense of shared responsibilities between private actors and the state authorities.[1771]

The 2003 Interinstitutional Agreement on Better Law-making defines co-regulation as:

> "*…the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations).*"[1772]

A variety of commentators have offered typologies of self- and co-regulation which chart regulatory approaches according to the degree of state involvement. This shall not be discussed further here.[1773] It shall be sufficient for the purposes discussed here that the difference between self- and co-regulation is that in the latter the state sets binding policy objectives

---

1767 Weber (n 265) 18–19.

1768 Cohen (n 19) 395–402. Cohen portrays the risks and disadvantages of self- and co-regulation in the information age in an almost interchangeable way.

1769 Senden and others (n 1654) 35–36.

1770 Cornils (n 481) 38–40. Cornils describes a scaled approach by which self-regulatory industry commitments, which failed regulators' expectations, are formalised and imposed by law. Economic actors are still left to organise compliance with the provisions. Irene Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 24, 6–7. Kamara identified differences of self- and co-regulatory approaches in European standardisation. See for a more general discussion: Michèle Finck, 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy' <https://papers.ssrn.com/abstract=2990043> accessed 3 August 2020. Marsden, *Internet Co-Regulation* (n 275) 51–70. Dimitrios Koukiadis, *Reconstituting Internet Normativity : The Role of State, Private Actors, Global Online Community in the Production of Legal Norms* (First edition., 2015) 63–64.

1771 Marsden, 'Guaranteeing Media Freedom on the Internet' (n 280) 82–86.

1772 Interinstitutional agreement on better law-making, OJ C 321/01 para 18.

1773 For examples see: Marsden, *Internet Co-Regulation* (n 275) 51–63; Senden and others (n 1654) 35–39; Saurwein, Just and Latzer (n 1656) 38.

through legislation. Private industry actors are then given the task to develop systems and measures to comply with these objectives. The state will finally be involved in approving, implementing, monitoring and enforcing the solutions drawn up by private actors. This is slightly distinct from the enforced self-regulation concept developed first by *Braithwaite*, where the state would have a mere approval, but no enforcement, and only limited monitoring duties.[1774] However, this "extension and individualisation of co-regulatory theory"[1775] is not considered substantial for the purposes discussed below and could be adjusted at a later stage if needed.

The following section gives a brief account of commonly voiced supportive and critical points of self- and co-regulation and their application to the internet.

a. Self-regulation

The prevalence of self-regulation on the internet has already been remarked on in Chapter 2. The tendency of the US Government to put the internet's infrastructural regulation to ICANN, a privately organised stakeholder organisation that relies on contractual arrangements, is just one aspect. It reflected a traditional cultural preference of self-regulation in the US. Through the influence of the cyberlibertarians of the 1990s, these self- or even autoregulatory structures have been extended to content regulation. This was certainly aided by the fact that the internet cuts across different jurisdictions with ease and determination. As a result, states have so far relied widely on private regulatory arrangements to address public interests when it comes to unlawful content online.[1776] Today, these structures are entrenched further by the private contractual arrangements between platforms and users. Content regulation, as shown in Chapter 4, has become predominantly a privately enforced matter in which the state has but limited power and influence. Current internet regulation emphasises freedom from the state, claiming that public interference into its contractual architecture is less efficient and not adapted to the needs of the contracting parties.[1777]

1774 Ayres and Braithwaite (n 39) 102–108.
1775 ibid 102.
1776 Wagner, *Global Free Expression - Governing the Boundaries of Internet Content* (n 136) 128–129.
1777 Koukiadis (n 1769) 284–285.

Yet, there are additional reasons for the reliance on self-regulatory models in today's internet and content governance. For one, today's regulators and enforcers face a capability challenge in enforcing against unlawful activity on the internet. This capability gap has been demonstrated in the sectoral analysis and case studies in Chapters 4 and 5. Regulators may not be prepared, staffed or budgeted to deal with the sheer amount of content, and the technical skills required to supervise and audit the automated decision-making procedures of online platforms.[1778] The supposed subjects of regulation are therefore readily brought back into the frame in order to help addressing concerns over unlawful content. Secondly, the internet introduces a new horizontal challenge that cuts across legal domains and nation states. The new nature of multi-sided global online platforms calls for innovative and interdisciplinary approaches, which often goes against the sectoral and specialised realm of traditional regulators.[1779] This has become apparent in the case studies on product and food safety enforcement. Specialised food scientists and technical engineers are not well set up to deal with assessing product risks and taking enforcement action on products sold online via marketplaces or social media platforms. Thirdly, public authorities can rarely match the 'discursive capacities'[1780] of (the internet) industry to assemble different stakeholders and shape policy debates and perceptions on a societal level. The extensive lobby activities of the internet's largest actors have been prominently noted.[1781] As a result, self-regulatory proposals and initiatives receive more coverage and thought than other policy approaches. Lastly, many European countries and varieties of capitalism have traditionally been embracing self-regulatory and other collaborative structures between state and industry. This is especially the case for

1778 Jason Freeman, 'Consumer Legislation and E-Commerce Challenges' (2015) 2 Rivista Italiana di Antitrust/Italian Antitrust Review 2 <http://iar.agcm.it/article/view/11380> accessed 19 September 2017; Cohen (n 19) 383–397; Leighton Andrews, 'Algorithms, Regulation, and Governance Readiness' in Karen Yeung and Martin Lodge, *Algorithmic regulation* (2019) 214–216. Spindler and Thorun (n 1689) 6. Deirdre K Mulligan and Kenneth A Bamberger, 'Saving Governance-By-Design' (2018) 106 California Law Review 697, 768–770. Cohen shows how regulator's capacities are being outpaced by "infoglut" and rapid technological change. Andrews describes a shortfall in governance readiness with regards to states' delivery and regulatory capacities where it concerns algorithmic regulation.

1779 Cohen (n 19) 375–387; Andrews (n 1777) 215. Goyens (n 1685) 202.

1780 Andrews (n 1777) 216.

1781 See for example: Tambini and Moore (n 232) 405. Zuboff (n 5) ll 2271–2343.

new and emerging industry sectors.[1782] *Marsden* states that self-regulation, together with state regulation, is as old as markets.[1783]

Self-regulation may therefore appear to be a natural choice for the internet. The European Commission's various initiatives and the marked preference for this kind of regulation in the ECD and the DSMD seem to support this. But self-regulatory models for the internet have also received mounting controversy.[1784] The previous sectoral chapters have outlined some of the flaws of self-regulation when it comes to content regulation and unlawful activity. One main criticism refers to a loss of democratic control, accountability and transparency where online intermediaries are left to regulate content under self-imposed rules and processes.[1785] This is of particular concern when public interests collide with private commercial objectives. Restricting unlawful content or risky, harmful behaviour will more often than not conflict with the business objective of maximising user traffic and data generation, and steer interaction. The less precise public interests are being articulated, the less likely self-regulation will achieve its objectives. Industry codes of practice, for example, are often too vague, with few tangible accountability and transparency provisions.[1786] In this game, commercial interests have so far prevailed, as the ongoing availability of unlawful content and the inefficacy of the self-regulatory initiatives discussed in Chapter 4 have shown. The far-reaching liability immunities for online intermediaries and the persisting ambiguities in this area make self-regulatory initiatives, which are already difficult to enforce legally, even less likely to be respected.[1787]

The efficacy of self-regulation is further dented by the gatekeeping powers of today's information intermediaries.[1788] Dominant market players have enhanced means to obscure irresponsible content management and risky design features of their services. They are able to exercise discreet

1782 Senden and others (n 1654) 20–30; Marsden, *Internet Co-Regulation* (n 275) 67–70. Senden describes marked self- and co-regulatory traditions in Germany, Italy, the Netherlands and the UK. Marsden identified Scandinavian and 'Rhinish' varieties of capitalism as conducive to co- and self-regulatory structures.

1783 Marsden, *Internet Co-Regulation* (n 275) 54.

1784 Spindler and Thorun (n 1689). Saurwein, Just and Latzer (n 1656) 42.

1785 Weber (n 265) 22; Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' (n 83) 223–225.

1786 Kleinsteuber (n 282) 66.

1787 Pasquale (n 19) 496. Saurwein, Just and Latzer (n 1656) 40–42.

1788 Helberger, Kleinen-von Königslöw and van der Noll (n 120) 50.

powers on platform participants because of the network effects they have created. Meanwhile, their considerable discursive capabilities and technological superiority infiltrate and influence the thinking and policy making of regulators, leading to "deep capture."[1789]

The current oligopolistic market structure, in which one or two major platforms hold sway over certain online service sectors (*Facebook* for social media and instant messaging, *YouTube* for video-sharing, *Amazon* and *Alibaba* for e-commerce, *Google* for search) means that self- or auto-regulatory 'solutions' by these players become the quasi-standard. There is little chance for regulatory competition, or a true, more open multi-stakeholder exchange.[1790] As self-regulation is not legally binding, it leaves the door open for black sheep to undermine standard practices.[1791] The weakest link argument is a particularly powerful one in the context of the global nature of the internet. It is supported by analysis made in Chapter 4 in the area of terrorist content or unsafe products. Smaller or less prominent platforms have attracted an increasing amount of unlawful activity as regulators focus on the dominant players. Meanwhile, the non-binding character of current industry agreements gives the state only limited room for effective enforcement. The general lack of transparency and democratic accountability of self-regulatory arrangements is only exacerbated by current market structures, fast-moving information technologies and the amount and speed with which online content is shared globally. The criticism of "privatised censorship" is therefore intrinsically linked to the self-regulatory practices of online platforms today.[1792]

b. Co-regulation

Co-regulation has been one proposed solution to counter the trend of free-wheeling private content regulation. The reliance on state-imposed regulatory objectives, on the one hand, and the freedom granted to platforms to devise adequate and accountable technical solutions, on the other, have been seen as an answer to the regulatory capability challenge while ensuring accountability and compliance with public interests. The above-men-

1789 Cohen (n 19) 376–378, 395.
1790 Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' (n 83) 222.
1791 Weber (n 265) 22.
1792 Cornils (n 481) 42.

tioned systemic approaches to online intermediaries, which rely on co-regulation, shall serve as examples for how a variety of experts have proposed to address this regulatory conundrum. For *Kleinsteuber*, a more appropriate term would be "regulated self-regulation." Compared to traditional "command and control" state regulation and to self-regulation, co-regulation is a relatively recent phenomenon.[1793] Originating in Australia, it has been discussed and subsequently adopted by national governments in Europe since the 1980s and 1990s. The EU has continued to support the use of self- and co-regulatory models as part of their better law-making agenda.[1794] This can, for example, be seen by the Principles for better self- and co-regulation as part of the EU's digital agenda.[1795]

Examples of co-regulatory approaches adopted by the EU include the previously discussed EU Food Safety and *New Approach* product regulation framework,[1796] or the REACH chemicals and environmental framework.[1797] In areas driven more by digital technologies, the media sector (AVMSD) [1798] or data protection (GDPR)[1799] are prominently cited examples for co-regulation. In all these areas, structured regulatory oversight authorities are in place at national and/or EU level, that monitor, enforce and audit compliance of industry's efforts to meet public interest objectives set by law.[1800] Co-regulation is seen as a more flexible and 'decentred' approach compared to command and control legislation, and a more struc-

1793 Kleinsteuber (n 282) 62–63; Marsden, *Internet Co-Regulation* (n 275) 54.

1794 European Commission, 'Communication: Better Regulation for Better Results - An EU Agenda - COM/2015/0215 Final' (2015) s 3.1. Colin Scott, 'Integrating Regulatory Governance and Better Regulation as Reflexive Governance' in Sacha Garben and Inge Govaere (eds), *The EU better regulation agenda: a critical assessment* (Hart 2018) 17–18.

1795 European Commission, 'The "Principles for Better Self- and Co-Regulation"' (*Shaping Europe's digital future - European Commission*, 22 August 2014) <https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation> accessed 4 August 2020.

1796 See also: Mark Dawson, 'Better Regulation and the Future of EU Regulatory Law and Politics' (2016) 53 Common Market Law Review 1209, 1231–1233.

1797 Carolyn Abbot, 'Bridging the Gap – Non-state Actors and the Challenges of Regulating New Technology' (2012) 39 Journal of Law and Society 329, 354.

1798 Cornils (n 481) 38–39. AVMSD 2018/1808 Recitals 12 - 14.

1799 Kamara (n 1769).

1800 Regulation (EU) 1025/2012 of 25 October 2012 on European standardisation 2012 (OJ L 316, 14112012) Article 5. With a possible qualification that the AVMSD supports co-regulation mainly in the area of traditional media regulation, while the measures for VSPs in Article 28 (b) would not (yet) squarely sit within that category.

tured and accountable solution compared to self-regulation. It answers to the demand for a more responsive regulation.[1801] This demand is created by new challenges in regulating in a world characterised by diverse, fast-changing business and social environments, information asymmetries as to the expertise needed to regulate effectively and various social actors that control and participate in regulation.[1802] Co-regulation is connected to other concepts commonly associated with responsive regulation, such as risk regulation, standardisation, corporate social responsibility or regulatory governance.[1803]

Co-regulatory solutions have several strengths that make them particularly suitable for addressing the challenges posed by new markets and technologies.[1804] First, the state and private actors share power in the regulatory process.[1805] Ideally, this power sharing acknowledges and exploits the intrinsic controls that these actors already have. A co-regulatory arrangement would install additional independent oversight mechanisms where there is a danger of conflict of interest and where public interests or fundamental rights are involved, e.g. ethical concerns in algorithmic content selection.[1806] Secondly, regulators can make use of the resources and the subject matter expertise of the regulated subjects.[1807] Moreover, the regulator will be able to acquire technical expertise through its involvement in monitoring and auditing compliance. This is one of the major obstacles today for embedding public values into technology design.[1808] Meanwhile, industry actors may get insight into the rationales and objectives that drive policy making. This process helps mitigate existing information asymmetries. Thirdly, co-regulatory systems are more flexible. Public – private ar-

1801 Ayres and Braithwaite (n 39) 102–109. It should be noted that Ayres and Braithwaite's distinction between co-regulation and enforced self-regulation is not followed here. For the purposes of this work, internal company compliance frameworks which are based on industry standards are treated as co-regulatory solutions.

1802 J Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 Current Legal Problems 103, 106–110.

1803 Marsden, 'Prosumer Law and Network Platform Regulation: The Long View towards Creating Offdata' (n 1750) 395. Ford (n 1656) 69–73. Koukiadis (n 1769) 66.

1804 Abbot (n 1796) 347.

1805 Koukiadis (n 1769) 63.

1806 Saurwein, Just and Latzer (n 1656) 41.

1807 Abbot (n 1796) 348.

1808 Mulligan and Bamberger (n 1777) 740–741.

rangements, such as standards, and regular contact between industry actors and regulators allow for adaptability to fast-paced technological and business environments. Regulatory disconnects can be detected in a timely manner.[1809] This flexibility extends also to the diversity of economic actors. A co-regulatory solution could for example allow for tailored content risk management solutions depending on online platform's business models, while respecting the underlying horizontal public interest principles.[1810] Fourth, the flexibility and adaptability allow for experimentation and the application of innovative policy solutions. This could be particularly useful in the diverse and multi-level regulatory space of intermediary responsibility. The rich experience from various best practices, national regulatory initiatives or industry solutions, is a fertile ground for policy experimentation[1811] and could be exploited through a co-regulatory approach. Fifth, enforcement is made easier and cheaper.[1812] Co-regulatory arrangements often lead to companies themselves establishing or being required to establish their internal oversight functions in the form of compliance officers or teams.[1813] This means the private sector will bear the majority of costs, while internal compliance functions still need to answer to public regulators. Lastly, co-regulation allows for the inclusion of various society stakeholders in the rule making process. Apart from industry and regulators, civil society, consumers or adjacent regulators can be brought into decision-making and oversight functions.[1814] At EU level, it may therefore be used to address allegations of democratic deficit or legitimacy gaps with which EU policy making has been plagued.[1815]

However, where the regulator tries to regain control, it needs to counter the pressures that have led to the emergence of self-regulatory models in

1809 Abbot (n 1796) 348.
1810 Finck (n 1769) 20.
1811 Wolfgang Kerber and Julia Wendel, 'Regulatory Networks, Legal Federalism, and Multi-Level Regulatory Systems' (2016) 13–2016 5–6 <http://ssrn.com/abstract=2773548> accessed 6 April 2017.
1812 Finck (n 1769) 21.
1813 The GDPR requires data protection officers, various health and safety regulations require the creation of health and safety officers, while in financial regulation compliance departments are responsible for various regulatory requirements such as anti-bribery, money-laundering or Ayres and Braithwaite (n 39) 105–107; Sean J Griffith, 'Corporate Governance in an Era of Compliance' (2015) 57 Wm. & Mary L. Rev. 2075.
1814 Marsden, 'Prosumer Law and Network Platform Regulation: The Long View towards Creating Offdata' (n 1750) 394–395.
1815 Finck (n 1769) 26–27.

the first place. How will the state design and structure a co-regulatory system that: formulates clear public policy objectives; introduces accountability into the secretive design decisions of private content governance systems; gives regulators technical and multidisciplinary expertise to effectively evaluate and verify responsible technology designs; and that re-introduces public legitimacy into the policymaking process?

These are questions that lead beyond the more structural connotations of the term co-regulation. Indeed, co-regulation calls up a whole host of other concepts of responsive regulation, such as governance,[1816] legal pluralism, compliance,[1817] standardisation, corporate social responsibility (CSR),[1818] duty of care[1819] or risk regulation.[1820]

II. Corporate (social) responsibility for online platforms

There is no authoritative or commonly agreed on definition of corporate social responsibility (CSR). Leaving the differences between national or international CSR commitments aside,[1821] it can generally be said that it means that companies take responsibilities for their impact on society, by ensuring that social, environmental, ethical and consumer concerns are incorporated in their business operations and strategy.[1822] The demand that online platforms act more responsibly with regards to the fight against unlawful content is increasingly linked to them embracing wider principles of CSR.[1823] Many of the popular platforms have become globally operating corporate actors. Even where they operate only out of one jurisdiction, their content is exposed to users worldwide. Their content management practices, however, are often competing with state regulation. This had led to calls for including internet intermediaries into international corporate responsibility frameworks to ensure their content management, informa-

1816 Marsden, *Internet Co-Regulation* (n 275) 55.
1817 Finck (n 1769) 17, 24.
1818 Spindler and Thorun (n 1689) 8–9, 22.
1819 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 236–238.
1820 ibid 243–244; Favro and Zolynski (n 1015) 4.
1821 John Gerard Ruggie, 'Multinationals as Global Institution: Power, Authority and Relative Autonomy: Multinationals as Global Institution' (2018) 12 Regulation & Governance 317, 317.
1822 European Commission, 'UCP Directive Guidance' (n 57) 63.
1823 Taddeo and Floridi (n 120) 1578.

tion access and privacy practices comply with (international) fundamental rights standards.[1824] Other have argued that the social responsibilities of platforms under local intermediary liability and data protection laws should be seen in conjunction with forward looking responsibilities to create conditions for responsible usage. This would result in a system of cooperative or organisational responsibilities that takes account of the gatekeeping and infrastructural powers of online platforms to enable responsible behaviours by their users.[1825]

CSR could be a tool that may guide internet intermediaries in the development of systems that safeguard users' fundamental rights.[1826] Others point to the fact that co-regulatory systems should be seen as a chance for online platforms to demonstrate their commitment to CSR principles.[1827] The above-mentioned Principles for better self- and co-regulation under the EU's digital agenda have arisen out of the EU's strategy on CSR. CSR could therefore be seen as one means to fill the *Durkheimian anomic space* created by the new Web 2.0 information intermediation practices and their wide reaching intermediary liability immunities. Active and transparent cooperation between state institutions and socially responsible enterprises,[1828] in this case, online intermediaries, along CSR principles could be a step to fill the current void of responsibility with new values when it comes to combating unlawful activity.

1824 Taddeo and Floridi (n 1014) 1579. Agnes Callamard, 'The Human Rights Obligations of Non-State Actors' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) 211–212 <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020. Such as in the Council of Europe, 'Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th Meeting of the Ministers' Deputies)'.

1825 Helberger, Pierson and Poell (n 68) 3–4.

1826 Tarlach McGonagle, 'The Council of Europe and Internet Intermediaries' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) 247 <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020.

1827 Spindler and Thorun (n 1689) 22.

1828 Senden and others (n 1654) 10–11. European Commission, 'Communication: A Renewed EU Strategy 2011-14 for Corporate Social Responsibility, COM/2011/0681 Final' (2011) para 4.3. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0681> accessed 6 August 2020.

III. Duties of care

The tendency towards formulating new duties of care for online platforms has been mentioned throughout the preceding chapters. Apart from being already an explicit policy option for Member States when regulating the responsibilities of online intermediaries under the ECD, it has been increasingly suggested by policymakers and academics. Duties of care are directly linked to obligations that platforms have as diligent economic operators. This has been confirmed by CJEU and national case law mentioned throughout this work. They may be a particularly useful tool for imposing an obligation responsibility[1829] on online platforms because of their link to negligence principles under various secondary liability doctrines in both civil and common law systems.[1830] It should be pointed out that the duties of care advocated here refer to the negligence, tort-based duties that some Member States already draw on from their ordinary law areas, or which are established through statutes in national and EU law. They should be distinguished from the methodological approaches developed by the CJEU when examining institutions' use of discretionary powers and compliance with the principle of proportionality.[1831]

Duty of care as a concept has been applied both by courts and as a principle in regulation. In both contexts the focus is decidedly procedural. Under a duty of care approach, courts will not look at the quality of a business decision but at the quality of the decision-making process.[1832] The principle of duty of care lends itself particularly well to proportionality assessments and the rights balancing exercises involved in these acts. It is helpful when evaluating whether the different factors involved in the decision-making process were adequately considered.[1833] This means a court will need to review facts, knowledge and the public and private interests at

1829 Naughton (n 6) 389.

1830 See Chapter 3

1831 Herwig CH Hofmann, 'Delegation, Discretion and the Duty of Care in the Case Law of the Court of Justice of the European Union' [2018] SSRN Electronic Journal 15–19 <https://www.ssrn.com/abstract=3169744> accessed 28 August 2018. Nevertheless, both notions of duty of care share the focus on procedural aspects, the consideration of (technical) facts and risk management principles.

1832 Robert J Rhee, 'The Tort Foundation of Duty of Care' (2013) 88 NOTRE DAME LAW REVIEW 61, 1147.

1833 Hofmann (n 1830) 18.

stake.[1834] Duty of care is therefore particularly well suited to more complex, highly technical situations which may not be solved by using traditional legal means, such as judicial review. However, it has also been shown that in the high volume, fast-changing and diverse area of intermediary liability courts may not be the most effective and best suited institutions to engage in duty of care reviews and establish standards of responsibility.[1835]

The advantage of statute-based duties of care is that they can bypasses potentially diverging, and even contradictory interpretations of national and ordinary law concepts of secondary liability or torts. They lend themselves to more complex technical areas where risks are dynamic and where prescriptive, rules-based requirements may fail to take account of the variety of possible threat scenarios. *Woods* describes the historical process of incorporating duty of care into statutes of common law jurisdictions, using the example of UK Health and Safety legislation.[1836] Duty of care principles, based on reasonableness or the Roman law concept of *bonus pater familias,* have also been applied in civil law countries[1837] and in EU law contexts in general. For example, under EU product safety law distributors have certain defined due care obligations with regards to products placed on the market by manufacturers.[1838] The duty of care is not always specifically indicated as such but often referred to as 'due care', 'reasonable measures', 'reasonable care', 'diligent behaviour' or ' professional diligence' related to certain threats or risks. This, however, also entails that parties with responsibilities engage in risk assessment exercises or demonstrate that they have sufficient knowledge and adequate processes in place to address risks. The GDPR,[1839] AVMSD,[1840] REACH[1841] or the EU Framework Di-

1834 ibid 16.
1835 Frederick Mostert, 'Free Speech and Internet Regulation' (2019) 14 Journal of Intellectual Property Law & Practice 607, 610; Finck (n 1769) 18. Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 232.
1836 Woods, 'The Duty of Care in the Online Harms White Paper' (n 794) 7–10.
1837 Valcke, Kuczerawy and Ombelet (n 551) 111.
1838 Decision 768/2008 Article R5.
1839 Regulation 2016/679 (GDPR) Article 35.
1840 AVMSD 2018/1808 Article 28b (3).
1841 Regulation 907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH 2006 (OJ L 396) Recitals 17 - 19.

rective on Health and Safety at Work[1842] establish such ongoing, dynamic responsibilities for economic actors. These responsibilities entail risk management procedures against broadly formulated public interest objectives or fundamental rights of employees or users. The AVMSD provides an example where these principles have been applied to VSPs, a certain type of hosting providers. The DSMD also relies to a certain extent on these principles by requiring OCSSPs to demonstrate that they have made best efforts in the prevention of unlicensed content on their platforms. When fixed in statutes, duty of care needs to be moulded into more structured frameworks. This is also necessary in order to reduce ambiguity and differences in interpretation and application that would ensue from tying duties of care to ordinary law principles. As has been shown in Chapters 2 and 3, the negligence-based duty of care concept is not equally recognised and applied in Member States legal systems. Risk regulation and standardisation provide more neutral and generic structural and procedural frameworks that are capable of ironing out these kinds of differences. These concepts shall be explored in more detail below.

IV. Risk regulation and compliance

The formulation of duty of care responsibilities through statutes is closely linked to risk (based) regulation. Risk regulation focusses on the control of risks, with a priority given to high risk activities of regulated entities. Compliance with set rules is of lesser importance.[1843] Risk regulation has emerged since the 1990s as part of a drive towards flexible regulation and regulatory governance.[1844] Regulators tried respond to the new challenges posed to state authority in a globalised, information society system in which policy-relevant knowledge is distributed throughout society (industry, technical experts, regulators) and held in epistemic communities. The state loses its central character as an epistemic authority[1845] as the focus of

1842 Council Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work 1989 (OJ L 183) Articles 5, 6, 9.

1843 Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd ed, Oxford University Press 2012) 281.

1844 Ford (n 1656) 60–74.

1845 Schepel (n 34) 25.

public policy changes from politics to technical expertise.[1846] Risk regulation addresses the state of uncertainty on the part of the regulator by requiring the firm to comply with regulatory objectives through defined risk management processes. It acknowledges that economic actors are best placed due to the control and ownership they have over their internal data and business processes to assess the risks related to their activities. Regulators have little knowledge initially of how disruptive innovations, such as the internet or digital technology, will affect public values. They also have no reference to assess the impact of regulation,[1847] nor have their functions traditionally required that they use ('big') data to measure compliance, or establish liability and conformity.[1848]

If a regulatory objective were that an e-commerce online platform does not facilitate the sale of trademark infringing goods while respecting sellers' freedom to conduct a business, then it would need to demonstrate whether and how its business model and technical architecture promote responsible seller behaviour. Secondly, the platform would need to demonstrate that is has internal controls in place to contain high risk activities that occur on the platform (such as seller onboarding due diligence, NTD systems, risk-based monitoring).[1849] Modern approaches to risk regulation would aim to produce decisional accountability, whereby economic actors will need to be able to demonstrate to regulators and other stakeholders that public values and interests are being respected and how this is done.[1850] For that to happen, regulatory risk management or risk-based approaches will be individualised at the firm level. They will need to be embedded in the technology and, for platforms, in the technical architecture and the algorithms that make content decisions. The regulated company would need to show that its design choices were done with public interest obligations in mind and with a view to contain any activities that pose a high risk to public values.[1851] That demonstration would entail technical

1846 Haas (n 38) 4–7. Nupur Chowdhury and Ramses A Wessel, 'Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance?' (2012) 18 European law journal 335, 337.

1847 Ford (n 1656) 186–191. Marsden, *Internet Co-Regulation* (n 275) 231–234.

1848 Zeno-Zencovich and Codiglione (n 1750) 54.

1849 Baldwin, Cave and Lodge (n 1842) 282.

1850 Bamberger (n 37) 684–685.

1851 Baldwin and Black note the move away of regulators from process/based controls to a focus on high risk activities or key problems. Robert Baldwin and Julia Black, 'Driving Priorities in Risk-based Regulation: What's the Problem?' (2016) 43 Journal of Law and Society 565, 568.

documentation, records of risk management procedures (risk identification, assessment and control), impact assessments and internal tests and audits of the internal processes. Risk regulation has been widely applied in the financial sector, in environmental management, but also in biotech, food and product safety regulation.[1852] In the digital technology area the GDPR[1853] and the Security of Network and Information Systems (NIS) Directive[1854] are prime examples for such risk regulation.

The demands of risk regulation have led to the emergence of compliance functions within companies. For one, statute may require such a function within a company. EU Anti-Money laundering legislation, the GDPR or Health and Safety legislations are cases in point that foresee 'responsible persons' or compliance officers for companies that engage in high risk activities. Secondly, large companies will not be able to run efficient regulatory risk management functions simply as part of their normal business teams. Compliance teams often need functional, financial and hierarchical independence within the company and develop their own technical expertise.[1855] However, the rise of automated compliance systems has somewhat worked against the fully independent compliance function.[1856] For Griffith "compliance is a de facto government mandate imposed upon firms."[1857] "It does what corporate laws' duty of care might have done."[1858] Thirdly, due to the complexity and the variety of risks, regulators often encourage or mandate the development of standards and automated reporting systems in order to effectively regulate firms. As a result, a whole new governance, risk and compliance (GRC) service industry has developed that offers the entire lifecycle of regulatory risk management, auditing and controls, and statutory reporting.[1859] For example, the best available technology safe harbour approach offered by *Helman and Parchomovsky*[1860] above would likely lead to the emergence of such a GRC system for compliance with copyright by online platforms.

1852 Cohen (n 19) 374, 393–394; Ford (n 1656) 103.
1853 Woods and Perrin (n 799) 23–24.
1854 Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union 2016 (OJ L 194) Articles 14 (1), 16 (1), Recitals 44, 46. 49.
1855 Griffith (n 1812) 2099–2103.
1856 Bamberger (n 37) 686–687.
1857 Griffith (n 1812) 2073.
1858 ibid 2113.
1859 Bamberger (n 37) 673–674, 689–702.
1860 Helman and Parchomovsky (n 309).

Another (optional) feature of risk regulation is the application of a precautionary approach. This principle was originally formulated in environmental legislation of the 1970s, but the practice of precautionary interventions dates further back.[1861] Under the precautionary approach a regulator should err on the side of caution if it cannot gain sufficiently reliable data or evidence in order to assess a risk. The approach is employed where certain activities may pose systemic risks that would cause irreversible damage, such as in the area of environmental and climate protection. On the downside, this approach may be highly costly and prevent innovation.[1862] *Woods and Perrin* suggest that it may be an appropriate approach in the regulation of social media platforms' content management systems. Evaluating the impact of certain harms is made difficult by constant change in algorithms and the fast proliferation of new features. However, the danger of significant damage to people and society calls for a precautionary application of regulation to these social media platforms.[1863]

In summary, risk regulation attempts to provide a framework for containing harmful practices in situations of uncertainty and rapid change. Responsible actors would need to put systems in place to identify and control the worst risks to public interests. Regulators, meanwhile, provide the public policy objectives and the risk management framework for economic operators. The interactions and the task sharing between regulator and industry make this predominantly an example of co-regulation.[1864]

Risk regulation still requires substantial investment and a culture change on the side of the regulator. For a start, regulators themselves need to acquire technical expertise and capabilities in order to be able to audit and assess risk management processes, control software or algorithms.[1865] Chapters 4 and 5 have exposed marked gaps in the analytical and delivery capacities[1866] of regulators in the areas of product and food safety and terrorist content. Meanwhile, as regards IP rights and hate speech such regulators are just emerging or not yet existent. Secondly, the mandate of (risk) regulators in the area of platform liability needs to be broadened and deepened. They should be empowered to seek cooperation with other regula-

1861 Mike Feintuck, 'Precautionary Maybe, but What's the Principle? The Precautionary Principle, the Regulation of Risk, and the Public Domain' (2005) 32 Journal of Law and Society 371, 374–375.
1862 Cohen (n 19) 394; Ford (n 1656) 190.
1863 Woods and Perrin (n 799) 10–11.
1864 Abbot (n 1796) 353–354; Marsden, *Internet Co-Regulation* (n 275) 232.
1865 Mulligan and Bamberger (n 1777) 768–770.
1866 Andrews (n 1777) 215–17.

tory agencies, solicit multi-stakeholder input from society and deepen their regulatory charge. The latter would include research, discursive capacities, legislative input, wider review powers and being subjected to judicial review.[1867] As will be described below, prominent failures in risk regulation are due mainly to regulators' inadequate oversight and misjudgement of their regulatory methods where complex, highly-automated compliance systems are being employed.[1868]

V. Standardisation

Technical standards, in the following referred to simply as standards, can be traced back over the last 150 years. As a response to the new complexity and diversity in production, the acceleration in technical innovation and the internationalisation of economies, both industry and governments sought to bring about more compatibility. Compatibility of products and processes was needed to accelerate industrialisation, innovation and efficiency gains in production.[1869] Standards arose out of bottom-up processes driven by industry. They are typically voluntary, but have also been imposed from above through legislation. Governments can, for example, lay down mandatory standards for certain products in order to meet requirements of public safety, security or other general interests.[1870] In the US, standards development is largely left to industry and market conditions, with minimum government oversight. Europe has traditionally favoured a more interventionist approach towards standards development by which governments may exert an oversight function and lay down regulatory objectives.[1871] However, entirely industry driven standards do also exist in Europe. As a purely industry driven exercise standards fulfil self-regulatory goals. Where the government is involved in setting the regulatory frame-

1867 For an excellent detailed account see Mulligan and Bamberger (n 1777) 760–768. and Andrews (n 1777).
1868 Cohen (n 19) 372–373.
1869 Stefan Timmermans and Steven Epstein, 'A World of Standards but Not a Standard World: Toward a Sociology of Standards and Standardization' (2010) 36 Annual Review of Sociology 69, 75–76.
1870 ibid 76.
1871 Jane K Winn, 'Globalization and Standards: The Logic of Two-Level Games' (2009) 5 I/S: A Journal of Law and Policy for the Information Society 34, 190.

works for standards development, this will result in co-regulatory structures.[1872]

The initial role of standards in ensuring interoperability and safety has expanded with globalisation and the above-mentioned normative competition exerted by transnational companies[1873] and their global value chains.[1874] Standards today still assure the seamless operation of globalised economic activity, but they have also taken on more social functions. Independent, third party certification of products and supply chains demonstrate compliance of private, transnational actors with wider ecological, social, human rights or technical values.[1875] For consumers, standards address the information asymmetries that exist in complex supply and information value chains by providing for traceability and transparency. For companies, they have become a substantial element of CSR efforts.[1876] As of today, standards are a pervasive feature of our societies that, whilst not easily visible to people in their daily actions, structure how they communicate, work or consume. Standardisation is a decidedly social act, and "an integral element of modern national political, economic and legal systems."[1877] At a global level, transnational standards have been described as the "hidden normative backbone of complex societies."[1878] This is in line with *Durkheim's* prediction that the division of labour and the internationalisation of industries and markets would itself form the basis for new rules and normative values.[1879] The state maintains a coordinative role as private actors from industry and civil society create consensual rules and technical requirements through standards. Standards can therefore be seen as filling the normative void created by increasingly specialised, knowl-

1872 Marsden, *Internet Co-Regulation* (n 275) 67–70; Finck (n 1769) 17–19.
1873 Teubner, 'Self-Constitutionalizing TNCs? On the Linkage of "Private" and "Public" Corporate Codes of Conduct' (2011) 18 Indiana Journal of Global Legal Studies 617, 633.
1874 Klaas Hendrik Eller, 'Private Governance of Global Value Chains from within: Lessons from and for Transnational Law' (2017) 8 Transnational Legal Theory 296, 315–316.
1875 Some of the numerous examples of certification schemes and standards, without commenting on their normative effect on supply chains and markets, are: the Forest Stewardship Council (FSC), EU energy consumption labels (Eco/labelling), organic product certifications, fairtrade certifications, CE product labelling.
1876 Eller (n 1873) 316–320.
1877 Winn (n 1870) 189.
1878 Eller (n 1873) 311–312.
1879 Durkheim (n 31) l 7029; Schepel (n 34) 14–15.

edge-based, global societies in which the state has lost its epistemic authority and needs to draw on social and economic actors.

Standards have some distinctive advantages over traditional command and control regulation, which would make them predestined as a regulatory and enforcement tool for a new intermediary responsibility system. First, efficient administrative rule-making in modern societies (in both the industrialised and the post-industrial information society) relies on technical and scientific expertise. Expertise resides outside government, with private actors in industry or civil society.[1880] In the area of intermediary responsibility, adopting a standards approach would take account of the fact that, across all content sectors discussed above, online platforms alone maintain the technical expertise to design responsible systems. Secondly, standards are flexible and can be modified according to technological and market changes. They can also be adapted to different platform business models and content areas.[1881] Although standards may still be not dynamic enough to keep pace with technology changes in the platform economy, some have argued that ICT standards development is generally nimbler than elsewhere.[1882] Thirdly, their cooperative character provides for opportunities of wide stakeholder inclusion. This is particularly the case where standards incorporate more procedural elements that can be linked to wider CSR efforts of companies.[1883] Given the wide societal interests served by online platforms, it is submitted here that a wide multi-stakeholder approach should be a decisive element of any standard developed in this field. However, it should also be pointed out that insufficient transparency and democratic legitimacy remain a significant critical point of standardisation. This is especially the case where this process relies on bottom-up, highly technical, self-regulatory arrangements that may be subject to regulatory capture.[1884] Fourthly, standards make it easier, cheaper and more predictable for economic operators to comply with more complex

1880 Van Gestel and Micklitz (n 1528) 154; Teubner (n 1872).

1881 Verbiest and others (n 315) 22–23.

1882 Winn (n 1870) 189.

1883 Eller (n 1873) 317.

1884 Abbe Brown and Rónán Kennedy, 'Regulating Intersectional Activity: Privacy and Energy Efficiency, Laws and Technology' (2017) 31 International Review of Law, Computers & Technology 340, 358; Van Gestel and Micklitz (n 1528) 152, 177–179; Herwig CH Hofmann, 'A European Regulatory Union - The Role of Agencies and Standards' in Panos Koutrakos and Jukka Snell (eds), *Research Handbook on the Law of the EU's Internal Market* (Edward Elgar Publishing 2017) 18.

technical requirements. Their unified nature also eases enforcement in an international environment.[1885] Lastly, in the EU, standardisation is already a tried and tested regulatory approach across a wide area of technical and economic fields and beyond.[1886] It has been prominently applied in two content areas that are affected by unlawful content online. Product and food safety regulation provide a chance to incorporate intermediary responsibility provisions and experiment with an already existing enforcement network.

In the EU, technical standardisation, and the use of harmonised technical standards in particular, has become a widely adopted regulatory approach of choice for a wide area of economic regulation since the 1980s. A procedural infrastructure in the form of standardisation and accreditation bodies has been in existence for over 20 years. In 2001, the EU confirmed that standardisation was seen as an effective way of achieving EU objectives.[1887] Since then, standardisation has been extended to a wide field of sectors, including service sectors and more horizontal areas with broader public interests, such as occupational health and safety. The EU solidified the procedural and political basis of standardisation in Regulation 1025/2012. It laid down transparency, participation and accessibility requirements for civil society and SMEs to account for the extension of standardisation into wider areas of CSR and social norms.[1888] In addition, it established an annual work programme for standardisation and vowed to expand it across other areas.[1889]

Standardisation received a further policy boost with the EU's 2016 Joint initiative on standardisation under the Digital Single Market. In this policy document, which is part of the EU's standardisation package, the EU commits to improving, amongst others, transparency and accountability of the standard setting process, the development cycle of standards and a push to use standards to support digitisation in Europe.[1890] The focus of European standards on ICT was confirmed in 2016 by the Communication on ICT

1885 Schepel (n 34) 67–70.
1886 ibid 71–72.
1887 European Commission, 'European Governance - A White Paper, COM(2001) 428 Final' (n 1764) 21.
1888 Regulation 1025/2012 Articles 5, 6; Schepel (n 34) 66–68.
1889 Regulation 1025/2012 Article 8.
1890 'Joint Initiative on Standardisation: Responding to a Changing Marketplace - Growth - European Commission' (*Growth*) <https://ec.europa.eu/growth/content/joint-initiative-standardisation-responding-changing-marketplace_en> accessed 29 August 2018 Actions 8, 9, 14.

Standardisation Priorities for the Digital Single Market.[1891] The EU acknowledged the increasingly fast change of digital technologies and the need for standards creation to adapt to this. It noted the new challenges that many new technologies, such as mobile apps or IoT pose on a horizontal level to security, privacy and user safety. It also noted the potential impact of standards on fundamental rights and the increasing controversy of access rights to standards.[1892] The annual work programmes on standardisation would adapt to the priorities set for the Digital Single Market. As an illustrative example, the EU requested the European standards organisations in 2015 to create a standard that would allow economic operators to develop, implement and execute privacy-by-design approaches demanded under the then proposed GDPR.[1893] The Commission asked that existing international standards such as ISO 9001 on quality management systems, ISO 27001/2 on information security management[1894] and European privacy risk management methodologies be considered in this process.[1895] It is suggested here that the EU could follow a similar approach if a new duty of care responsibility standard was to be made mandatory for online intermediaries.

The reliance of the functioning of the internet on standards needs no further mentioning. These standards have always been highly technical in nature. Standard setting bodies, such as the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C) were dominated by engineers and other technical experts. Butn as infrastructure regulation is being subsumed by content regulation, internet standard setting has also been increasingly invaded by content issues. Digital rights management, data protection and fears of censorship are more socially based, normative concerns that have found their way into these predominantly technical cir-

1891 European Commission, 'Communication: ICT Standardisation Priorities for the Digital Single Market COM(2016) 176 Final' (n 1696).

1892 ibid 3.

1893 Regulation 2016/679 (GDPR) Articles 25 (3), 42, 43.

1894 'ISO - ISO 9000 Family — Quality Management' (*ISO*) <https://www.iso.org/iso-9001-quality-management.html> accessed 11 August 2020; 'ISO - ISO/IEC 27001 — Information Security Management' (*ISO*) <https://www.iso.org/isoiec-27001-information-security.html> accessed 11 August 2020.

1895 Commission Implementing Decision on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management - C(2015) 102 final 2015 (M/530) 5–6.

cles of internet standard making bodies.[1896] The debate over the involvement of ICANN, the infrastructural guardian of the internet, in copyright enforcement is just one proof of this tendency.[1897] Technical standards of the internet, however, are able to address the increasing policy attentions and accommodate forum shifts. Yet, the balance needs to be carefully managed. As shown by *Harcourt et al* the work of technical standards bodies has been influenced through participation by society. Digital rights activists have been involved in protocol management to address the issue of user tracking and state surveillance, although their influence remains constrained.[1898] Overall, states have progressively ceded more formal involvement in policy matters to more informal participation in international standards fora without however relinquishing influence, which may pose additional challenges for democratic accountability.[1899] Despite these risks, this shows that a technical standardisation approach in the area of intermediary responsibility would fit into the wider regulatory structure of the internet. In addition, if the EU were to drive a wide stakeholder approach, this could go some way in addressing the current imbalances of making public interests and fundamental rights heard more equitably in standards development.

3. Application to a new intermediary responsibility framework

The approaches and policy tools outlined above will be an integral part of the online intermediary responsibility framework for unlawful content proposed hereafter. The suggested model will rely on co-regulation. The regulator would outline responsibilities through the definition of key harms or threats that touch on the public interest and fundamental rights. The responsibilities would translate into more defined duties of care that follow a risk-based approach. Compliance with these responsibilities would be certified through voluntary, harmonised standards.

1896 Alison Harcourt, George Christou and Seamus Simpson, *Global Standard Setting in Internet Governance* (First edition, Oxford University Press 2020) 5–6, 87–88. They describe how copyright protection has found its way into the World Wide Web Consortium (W3C) standard body. Efforts to use ICANN as an enforcer in the area of copyright are another example: Bridy (n 276).

1897 Bridy (n 276).

1898 Harcourt, Christou and Simpson (n 1895) 175–188.

1899 ibid 211, 236–237.

In the below summary the interaction between the different tools will be briefly outlined. Self-regulatory approaches have until now not been effective in fighting the ongoing problem of unlawful content on online platforms and intermediaries. This has been demonstrated for all content sectors above throughout Chapter 4. It is therefore appropriate to step up public involvement, as was done for example though the AVMSD. Co-regulation provides a more robust structure that gives the public sector necessary leverage. Lawmakers will set clear public policy and fundamental rights objectives through law and put regulators in charge of coordinating, supervising, auditing and enforcing compliance with these goals. The more structured and mandated cooperation that is characteristic of co-regulation is also better suited to answer to the demands for a cooperative responsibility of all stakeholders in the process of online intermediation.[1900] This reflexive process goes also a long way in addressing the current governance readiness gaps of public authorities when it comes to complex technological problems, and algorithmic systems in particular.[1901] It is also capable of being more accountable and transparent than pure self-regulation. Finally, the European technical standardisation process favoured here takes place in a co-regulatory setting. Meanwhile, both co-regulation and standards have the potential to address the diversity in the platform economy and the fast pace of technological change.

The proposed model will define responsibilities that follow the formulation of precise harms or threats to public interests and fundamental rights that are caused by various types of unlawful content on online platforms. The gradual move away from intermediary liabilities towards responsibilities has been in the making for several years.[1902] This was initiated by courts through e.g. the diligent economic operator principle, or the application of various negligence standards of secondary liability at Member State level. EU and national lawmakers have increasingly embraced this move over the last five years. The EU Communication and the subsequent Recommendation on enhanced responsibilities for online platforms attest to this.[1903] The responsibility framework also lends itself to wider incorporation into the CSR principles that acknowledge certain fundamental

1900 See for example: Helberger, Pierson and Poell (n 68).

1901 Andrews (n 1777) 210–223. Governance readiness comprises the delivery, regulatory, coordinative, analytical and discursive capacities of regulators.

1902 Frosio, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (n 1742).

1903 European Commission, 'COM (2017) 555 Final' (n 69) 2; European Commission, 'C(2018) 1177 Final' (n 8).

rights obligations of transnational corporations, of which the leading online intermediaries are prominent examples. Finally, both risk regulation and standards put an emphasis on proactive, responsible conduct by online platforms. The formulation of responsibilities directly shapes the definition and structuring of risks and risk management approaches.[1904] In addition, responsibility is more adapted to the multilevel and multi-actor field of intermediary liability, which is characterised by uncertainties. As a framework it is better suited to enable the emergence of standards and duty of care obligations than the more reactive and rigid ordering model of liability.[1905]

Duties of care are a fitting concept to structure and circumscribe the responsibilities of internet intermediaries. They are rooted in a more defined legal setting which is linked to negligence, although certain ordinary law differences remain at national level. Duty of care lends itself to highly technical and complex activities that are difficult to monitor with traditional legal tools.[1906] However, in order to prevent resorting to different national negligence approaches of secondary liability it is important to construct an independent duty of care and responsibility system. Risk management and technical standards could provide the frame for such a system that bypasses the risk of national divergence.

Like duty of care, risk regulation and risk-based approaches correspond to situations that deal with a high amount of uncertainty and that require a flexible and reflexive approach.[1907] Standards, on the other hand, formalise and structure risk management approaches, technical specifications and requirements based on multi-stakeholder input.

These concepts, applied to a new intermediary responsibility approach, all fit into the wider context of responsive or flexible regulation, that is associated with regulatory governance. They answer to the multi-level regulatory nature of the EU and the particular challenges in the area of intermediary responsibility. The gravity of potential harms and rights at stake necessitates multi-stakeholder involvement as well as more robust means for public intervention and goals setting. At the same time, a certain level of flexibility is required to account for the diversity of economic platform models and the types of harms or threats at stake.

1904 Baldwin and Black (n 1850) 578–579.
1905 Eller (n 1873) 324–327.
1906 Hofmann (n 1830) 18.
1907 Ford (n 1656) 69–73.

I. Risks and pitfalls of flexible regulatory tools

However, the tools and approaches mentioned above also share some common criticisms, which shall be discussed here. First, the lack of democratic legitimacy and procedural transparency are commonly voiced criticisms of co-regulatory arrangements. This extends to those systems that involve risk regulation and standard setting through highly technical and closed committees of specialists. This has been partly demonstrated in the above section on standardisation. Although this is an even larger problem in self-regulation, where public oversight is even less pronounced, it remains a real risk in co-regulation.[1908] This is particularly true where standards are driven through a bottom up approach and where government involvement remains limited.[1909] While *Marsden* suggests that this legitimacy gap is inherent in internet regulation, where technology and globalisation heavily favour the influence of corporations,[1910] co-regulation could also provide the answer to the problem. As regulators oversee the standard making process they could impose regular public reporting and disclosure requirements and actively promote the participation of civil society.[1911]

Secondly, the legitimacy problem is closely linked to the phenomenon of regulatory capture. As regulators work in close cooperation with industry during standard-setting and also in defining risk-based approaches, they may be drawn in by the latter's preoccupations and concerns. As a result, the regulatory responses risk being more tilted towards the interests of industry than public interests or fundamental rights. This is a particular problem in networked and technology-oriented settings[1912] and could therefore be a risk of the regulatory framework proposed here. Although this, too, may be a dilemma inherent in any co-regulatory standard devel-

1908 Marsden, 'Guaranteeing Media Freedom on the Internet' (n 280) 219; Regulation 1025/2012 Articles 5 - 8. This problem was implicitly addressed through these articles, which set the path for broader society stakeholder involvement in standard making and in the accessibility to standards. Spindler and Thorun (n 1689) 12.

1909 Brown and Kennedy (n 1883) 358.

1910 Marsden, 'Guaranteeing Media Freedom on the Internet' (n 280) 11–12.

1911 Finck (n 1769) 27. Spindler and Thorun (n 1689) 17. A first step was made with the Technical Standards Regulation, which requires that standardisation organisations encourage and facilitate participation of society stakeholders in the standardisation process.

1912 Cohen (n 19) 395.

opment process, one answer could be to decentre policy making and involve civil society groups in third party monitoring.

Remedying the two above risks through transparency, disclosure and third-party oversight are however no trivial tasks in the area of internet content regulation. More often than not, transparency and reporting requirements are executed as a lip service, resulting in disclosures that are politically invisible or insufficiently clear and convoluted. The disparate nature and selective detail of many transparency reports has been shown in the sections on hate speech or IP infringements in Chapter 4. The perceived irrelevance for users may then result in a subversion of public values.[1913] This is particularly true in the area of algorithmic regulation and machine learning systems. To address this risk, standard setting in this area should include requirements of disclosure, for example of information about data that was used to train algorithms. This would allow researchers to reproduce the programming of machine learning systems used by platforms for content moderation.[1914]

Third, regulators need to close the capacity or governance readiness gaps that currently hinder effective participation in policymaking, supervision and enforcement.[1915] Past failure of regulators to follow up and adequately audit technical systems, software and risk management processes have led to spectacular failures in self- and co-regulatory systems. One of the more recent prominent examples of failure in regulation through technology was the 2015 *Volkswagen* emissions software scandal.[1916] Regulators simply did not have the capabilities to detect and prove the fraudulent manipulation of the company's emission testing software that gamed regulatory requirements during a span of 6 years. This underlines the risks of compliance technologies, where compliance certification is left primarily to private entities. A powerful and technologically savvy company like *Volkswagen* was able to influence the control technologies. The fraud was eventually proven by independent researchers.[1917] On the one hand, the danger here would be, for example, that, first, a *New Approach* style certification system for algorithmic software that is supposed to mitigate the risks of unlawful content propagation could be gamed by one or several of the few, large platforms. Secondly, the manipulation is then missed or acquiesced

1913 Mulligan and Bamberger (n 1777) 776–780.
1914 ibid 780–782.
1915 ibid 759–768; Andrews (n 1777) 214–217.
1916 Mulligan and Bamberger (n 1777) 718–719.
1917 Cohen (n 19) 372–373.

to by the private entity that is appointed to audit or certify the software or system. On the other hand, if a regulator is not capable of understanding, evaluating and auditing software for the various algorithmic harms that content management systems may present, the regulatory objectives may be missed. Evidence of these harms is, however, emerging more strongly.[1918] While, aside from algorithm review, investigative techniques exist to identify and evaluate these harms (e.g. black box tinkering[1919] or the above-mentioned computational reproducibility[1920]), regulators need to be able to understand and apply them. There is a clear need for regulators and policy makers to go beyond their traditional remit and understand algorithmic decisions, because the data analytics behind them, are, in the end, inherently value-ridden.[1921] Regulators need to be able to decipher and evaluate these values against public interest principles.

This also means that regulators need to be able to function in true networks. Assembling different public actors in the multi-level sectoral structure of certain content sectors within the EU may not be enough. Horizontal, more holistic cooperation is also required. Pulling together experience from fields in hate speech, economic rights, consumer and data protection and competition law may produce useful synergies. This kind of cooperation through regulatory networks is particularly useful where, as in the area of platform responsibility, regulators and enforcers may have strong sectoral competencies, but where operational capacities are limited.[1922] This regulatory gap has been shown in the area of product and food safety enforcement. Here, a more holistic and diagonal exchange of information and training would arguably help regulators in their regulatory delivery capacities *vis-à-vis* online platforms. It would also help address the challenge of the 'diagonal integration' of today's leading online platforms.[1923]

Fourth, standardisation and co-regulatory arrangements may pose competition problems. If private standard setting bodies are dominated by

1918 Andrews (n 1777) 210–213.
1919 Maayan Perel and Niva Elkin-Koren, 'Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement » Florida Law Review' (2017) 69 Florida Law Review <http://www.floridalawreview.com/2017/black-box-tinkering-beyond-disclosure-algorithmic-enforcement/> accessed 11 April 2019.
1920 Mulligan and Bamberger (n 1777) 782.
1921 Vincenzo Zeno-Zencovich, 'Legal Epistemology in the Times of Big Data' in Ginevra Peruginelli and Sebastiano Faro (eds), *Knowledge of the law in the big data age* (IOS Press 2019) 4.
1922 Kerber and Wendel (n 1810) 6.
1923 Tambini and Moore (n 232) 399–401.

large, oligopolistic market players, there is a risk that standards are designed in such a way that they pose entry barriers for smaller, new competitors.[1924] This would be a real risk, if dominating platforms were, due to their technical and economic capacities, able to dictate discussions in standard setting fora. The Chapter 4 sections on copyright and trademarks have demonstrated that *Google* has, for example, become a leader in the development of content filtering technologies for copyright. *Amazon* is currently becoming a major (holistic) fraud detection service provider in the platform economy. The leading online platforms have superior capacities in this regard due to the fact that they can rely on vast amounts of user and traffic data, have formidable analytical and software development capacities and huge financial resources. Care would need to be taken that their technical and economic superiority does not lead to the development of standards that entrench their power further. Meanwhile, it is a fact that co- and self-regulatory institutional arrangements work most smoothly and are most stable when they rely on cooperation by oligopolistic market players.[1925] The temptation is that regulators become complacent with such seemingly steady and well-oiled arrangements.

Fifth, co-regulatory set ups, and *New Approach*, or *NLF* style, harmonised standards have faced more recent challenges regarding their constitutionality and the impossibility of judicial review.[1926] Harmonised standards, even under the current European approach, are still privately drawn up norms that enact public interest principles. Taken to the extreme, states could set up *Potemkin* regulators that pretend to perform regulatory supervision and enforcement of privately set up mandatory standards.[1927] Meanwhile, courts would find it difficult to review standards, first, due to their private nature and, secondly, because of their highly technical features.[1928] Until recently, the legal nature of technical standards and the institutional framework surrounding them was unclear. Since standards are not part of the public law body, the decisions of certification bodies had not been sub-

1924 Graz (n 1530) 79–80; Eller (n 1873) 327.
1925 Marsden, *Internet Co-Regulation* (n 275) 225.
1926 ibid 224; Galland (n 1527) 372–374. Spindler and Thorun (n 1689) 21. Van Gestel and Micklitz (n 1528) 151. LAJ Senden, 'The Constitutional Fit of European Standardization Put to the Test' (2017) 44 Legal Issues of Economic Integration 337, 342–348.
1927 Marsden, *Internet Co-Regulation* (n 275) 224–225.
1928 Harm Schepel, 'The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law' (2013) 20 Maastricht Journal of European and Comparative Law 521, 533.

ject to judicial scrutiny. Moreover, access to technical standards documentation is not free. Their location in "legal no man's land"[1929] has, however, been increasingly challenged. As harmonised standards have become an important part of the European regulatory space, they have ascended to become quasi law, but without sufficient constitutional safeguards attached to it.[1930] In *Fra.bo* the CJEU found that a private certification body of a widely applicable industry standard for water systems exercised *de facto* powers to regulate market access. Its decision affected therefore the economic freedoms under the EU Treaties.[1931] The tendency of submitting private regulation of the *New Approach* style to EU fundamental rights principles found its continuation in the more recent rulings in *Schmitt* and *James Elliott.*[1932] In *Schmitt*, the CJEU found that a consumer, who had been damaged through fraudulent breast implants, could have legal recourse against a private national certification body *(TÜV Rheinland)* because the latter owed a duty of care to consumers.[1933] In *James Elliott*, the CJEU judged that an European harmonised standard for construction products, in this case the composition of asphalt, was part of the EU body of law. Although a private law instrument, the harmonised standard enacted EU law. Harmonised standards have a public legal effect under the *New Approach* and they are published in the EU's Official Journal.[1934] This trend of the constitutionalisation of EU private regulation[1935] just outlines the democratic legitimacy and accountability challenges that this regulatory instrument has been facing.[1936] On the other side, increased constitutionalisation may also risk annihilating the distinct advantages of this type of regulation and reduce its appeal to industry and regulators.[1937]

1929 Van Gestel and Micklitz (n 1528) 150.
1930 Senden (n 1925) 351–352.
1931 *Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) — Technisch-Wissenschaftlicher Verein, C-171/11* [2012] EU:C:2012:453 (CJEU) [26–31].
1932 Paul Verbruggen and Barend Van Leeuwen, 'The Liability of Notified Bodies under the EU's New Approach: The Implications of the PIP Breast Implants Case' (2018) 43 European Law Review 394, 407–408.
1933 *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH*, [2017] EU:C:2017:128 (CJEU) [47].
1934 *James Elliott Construction Limited v Irish Asphalt Limited, C-613/14* [2016] EU:C:2016:821 (CJEU) [34–42].
1935 Verbruggen and Leeuwen (n 1931) 408.
1936 see also: Senden (n 1925).
1937 Schepel (n 1927) 533.

C. Primary and secondary responsibility and the sanctions regime

Chapter 4 has shown that sectoral attempts at reforming the current intermediary liability system have brought differing results. In copyright, non-diligent OCSSPs will be directly liable for copyright infringements. In trademark law, national courts have started to develop arguments for finding vertically integrated online marketplaces primary liable. Meanwhile, in speech related acts primary liability has been widely rejected by both courts and legislators, in favour of broader negligence-based duty of care approaches. Likewise, in product and food safety law, online intermediaries are generally not defined as economic operators with direct responsibilities. It is not immediately clear how a new approach towards platform responsibility can reconcile these different tendencies, nor whether it should.

The moral difficulties of making third parties directly responsible for the unlawful actions of others have been outlined in Chapter 3. This work sides with those that argue that *in principle* intermediaries should not be made primary liable for the action of others. Responsibilities, whose breach result in negligence-based, secondary liability would therefore be the preferred policy option. On the other hand, it has also been shown that some of the vertically integrated and intrusive business practices of platforms do indeed affect the substantive provision of the legal acts that regulate certain content. Apart from copyright, the commercial communication criterium in trademark law is one such example. Where platform intermediation affects the substantive law of the content/service that has been made accessible, primary liability would therefore appear to be a justifiable option. This could even be extended to product law, where failure on the side of online marketplaces to provide traders with the technical facilities to comply with statutory labelling and information requirements could result in direct liability. Meanwhile, for speech acts, the platform's activity of distribution or amplification does not affect the (il)legal nature of the content. Therefore, primary liability for defamatory and hate speech acts or terrorist offences would seem excessive.

It is submitted here that it would be too rigid in the context of the diversity of content and related laws to mandate either a full secondary or a full primary liability approach. The fluid lines between primary and secondary liability are likely to continue as business models and technologies evolve.[1938] Instead, this work argues for a special regime based on negli-

1938 Lipton (n 287) 1347; Assaf Hamdani (n 304) 106–107.

gence (linked to duty of care obligations). Negligence could, however, trigger (harmonised) primary liability where EU sectoral law provides for this, i.e. the DSMD. As shown in the copyright section in Chapter 4, the DSMD may well lend itself to a negligence-based duty of care assessment. In fact, the "best efforts" concepts can be applied to a risk-based duty of care standard).[1939] Where sectoral provisions do not foresee primary liability, a separate sanctions regime would be applied. The GDPR could serve as an example for the imposition of administrative fines and penalties.[1940] Alternatively, the regime would trigger secondary liability which would fall back to the provisions provided in national laws of Member States. In view of the disparate nature of the secondary liability regimes and their enforcement, this solution is, however, considered counterproductive.

D. A co-regulatory duty of care based on harmonised technical standards

1. Introduction

The following proposal sketches out a mandatory duty of care responsibility that follows a risk-based approach and relies on the (technical) standards system used under the *New Approach*. The focus of this proposals is on a) structuring the risk-based approach and b) how a risk management standard should be tied to a horizontal duty of care in legislation.

First, the methodological reliance on the *New Approach* and technical standard is influenced by the early elaborations of *Verbiest and Spindler* in their 2007 Study on the Liability of Internet Intermediaries for the European Commission, and the risk management approach first proposed by *Kempel and Wege* in 2010.[1941]

1939 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 (3), Recital 66.Chapter 4 C 4

1940 Regulation 2016/679 (GDPR) Articles 83, 84.

1941 Verbiest and others (n 315); Kempel and Wege (n 16). This was initially picked up by this author in his LLM Dissertation, written in 2012 at the University of Edinburgh: Ullrich, 'Online Intermediaries' Liability 2012' (n 17) 28–29 and subsequently refined by applying the principles of Transaction Risk Management in anti-money laundering: Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747).

Secondly, *Helman and Parchomovsky's* suggestion of a best available technology safe harbour for copyright infringements has been inspirational.[1942] The flexibility of such an approach, coupled with the best available technology standard that would be vetted and approved by a public body, has much in common with the standardisation solution offered here. The idea of creating a market for independent filtering service providers and the creation of a centrally managed copyright database also go a long way in pushing for public accountability and the respect of fundamental rights.[1943]

Thirdly, the more recent proposal of *Woods and Perrin*[1944] for a statutory duty of care has helped to validate and further improve on the framework suggested below. The definition of distinct harms by *Woods and Perrin* has helped to solve the question whether a framework should be structured by content area or type of intermediary. The harms-based approach will help platforms covered by the regulation to focus on the most important question: how to design their business models and technologies in a responsible way that pre-empts and eliminates the most egregious harms that users still risk to encounter on many online platforms today. In addition, *Helberger et al's*[1945] distinction of prospective and retrospective (cooperative) responsibilities have led to an adjustment of the risk assessment framework.

2. Changes to the ECD's online intermediary liability framework

The proposed scheme would radically change the current ECD intermediary liability provisions. First, the distinction between passive and active intermediaries would be removed. It has been shown throughout this dissertation that this distinction is outdated for today's information hosts. Courts have been grappling with the concept and a wide array of stakeholders have likewise questioned its relevance in the era of Web 2.0. Secondly, the actual knowledge standard, which is connected to the reactive concept of liability, would not be carried over into the new framework. Uncertainty (of knowledge and information) is a central element in risk as-

1942 Helman and Parchomovsky (n 309).
1943 ibid 1221–1226.
1944 Woods and Perrin (n 799).
1945 Helberger, Pierson and Poell (n 68).

sessment.[1946] Responsible platforms should do everything that can be reasonably expected of them to attain knowledge and data to assess the risk of the harms defined in legislation. Where such knowledge is not available, the risk assessment should lead the platform to take appropriate mitigation or precautionary measures. Thirdly, the new framework eschews the general monitoring prohibition of Article 15 ECD. It has been demonstrated that the definition of general monitoring remains unclear. It is suggested that this ambiguity will not go away with the ongoing evolution in technology. On the other hand, the protection of privacy, freedom of expression and other fundamental rights, can and should be effectively ensured through (algorithmic) governance, risk management and due process measures that are attuned to the particular harm in question and incorporated in the duty of care standard. In escalated cases, courts would conduct the balancing exercises and provide further guidance. It has been demonstrated and argued here that courts are able to conduct these balancing exercises without having to resort to the blanket prohibition of Article 15 ECD. This is supported by the view that the current use of Article 15 ECD presents an over-emphasis of free speech over other fundamental rights and harms, which sits uncomfortably with the European tradition of more equitable fundamental rights balancing.[1947] Lastly, the framework moves away from a liability to a responsibility regime. This also means that a "Good Samaritan" protection, as demanded by some for the EU,[1948] does not fit into such a new framework, which rests on positive responsibilities and does not see online platforms as neutral bystanders whose proactive measures are caritative acts that soften the harmful impact of their own systems.[1949] There is no single argument for broader responsibilities of online platforms. This work should have demonstrated that besides the purely

1946 European Commission, 'EU General Risk Assessment Methodology (Action 5 of Multi-Annual Action Plan for the Surveillance of Products in the EU (COM(2013)76))' (European Commission 2015) 14.

1947 Smith, 'Enforcement and Cooperation between Member States' (n 684) 33.

1948 Joan Barata, 'Positive Intent Protections: Incorporating a Good Samaritan Principle in the EU Digital Services Act' (*Center for Democracy and Technology*, 29 July 2020) <https://cdt.org/insights/positive-intent-protections-incorporating-a-good-samaritan-principle-in-the-eu-digital-services-act/> accessed 14 October 2020; Sartor (n 236) 31. Tambiama Madiega, 'Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act : In-Depth Analysis.' (European Parliament 2020) 18 <https://op.europa.eu/publication/manifestation_identifier/PUB_QA0420239ENN> accessed 14 October 2020.

1949 Smith, 'Enforcement and Cooperation between Member States' (n 684) 32–33.

economic reasons of the cheapest cost avoider, online platforms have become gatekeepers that occupy critical positions in the internet's informational and physical architecture. This, and their role as quasi-public spaces for large swathes of the world's population, confer on them also positive moral responsibilities to prevent harms that impact public interests and fundamental rights.

This is the suggested definition of online intermediaries to which this regime would apply:

> *Any information society service providers whose activity consists of the storage of information provided by a recipient of the service, whereby the recipient of the service is acting not under the authority or the control of the provider.*

It should also be noted this regime would not apply to IAPs. It is suggested that the current regime of the ECD's Article 12, which has been progressively re-interpreted and adapted by courts, is fit for purpose. Likewise, the caching provision in Article 13 would also be left untouched by the new framework. In addition, the special position of search engines should be considered and result in a modified, regime that takes account of the essential functions that these intermediaries have for the functioning of the internet.

Finally, the exponential impact of large, dominant platforms and intermediaries (*GAFAM*) in the area of content management has been repeatedly stressed. Due to time and space limitations, this work does not venture to develop a special regime of stricter duties of care for these players. Nevertheless, the creation of such an extra regime, which is considered by an increasing number of scholars and has also been included in the proposals of the Commission's Digital Service Act package, is expressly endorsed.[1950] The approach presented here could thus be adapted in order to enhance certain risk management and transparency obligations of these dominant platforms.

1950 Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' (n 83) 232 236; De Streel and Husovec (n 83) 45–46; Molly K Land, 'Regulating Private Harms Online: Content Regulation under Human Rights Law' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) 304–305 <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020.

3. Sectoral flexibility – the harms under a horizontal framework

In a previous version of the system proposed here specific duties of care were tied to different platform business models.[1951] The idea was that certain types of platforms were subject to specific 'sectoral' violations. UGC platforms were linked to specific duties in the area of copyright; online marketplaces to trademark violations; social media to hate speech and violence, and news portals (with comment functions) also to hate speech and propagation of violence. This system was open ended for new types of platforms and harms.

The harms approach suggested by *Woods and Perrin*,[1952] provides a simpler and at the same time more encompassing solution. The harms would be picked up through existing or future sectoral legislation. For example, in the area of hate speech the AVMSD Article 28b already sets out duty of care style obligations for VSPs. This could be complemented or replaced by reference to a duty of care standard for the harms addressed by this directive. This standard could then also be picked up by other sectoral provisions that address hate speech or the protection of minors, and which do not specifically address VSPs. The same could be done in the area of copyright for OCSSPs, where the best efforts mentioned in Article 17 DSMD could be supplemented or replaced by reference to a duty of care (technical) standard. In the same vein, IPRED could be amended to reference this standard for intermediaries in areas of IP law not covered by the DSMD. Likewise, the TERREG proposal and Regulation 2019/1148 on marketing and use of explosive precursors could reference a duty of care (technical) standard designed to address the specific harms caused by terrorist content or activity. The same goes for the MSR in the area of product safety, and selected regulations within the EU Hygiene package for the area of food safety. An illustration of such a sectorally adaptable system can be found in ANNEX II.

Meanwhile, the reformed ECD or a future DSA would serve as a framework directive or regulation. A framework directive/regulation is an EU instrument that establishes general (usually minimum) principles and policy

1951 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 249.

1952 Woods and Perrin (n 799) 35–40. Saurwein, Just and Latzer (n 1656) 38. are also proposing a harms based approach, but focus mainly on the governance of algorithms.

objectives for a broader legal area.[1953] However, it leaves flexibility to EU or national lawmakers to define stricter or deviating standards in *lex specialis* for specific sectors of the wider area covered by the framework legislation. As an example, the E-Privacy Directive (2002/58) is *lex specialis* to the GDPR in that it specifies the data protection rules applying to electronic communications.[1954] The GPSD and the MSR are framework provisions in the area of product safety and its enforcement, while sectoral provisions, such as the Toy Safety Directive, would lay down *lex specialis* where it concerns the specific obligations of manufacturers or distributors for the making available of toys on the EU market. Under this approach, the new EU act on digital services would establish the kind of harms and principles that a new duty of care responsibility system for online intermediaries would address. It could mention the kind of harms to which duty of care standards for information host would apply. The harms would then be linked to the sectoral acts, which contain reference to specific duty of care standards.

Below is a non-exhaustive proposal of overarching harms and some specific sub-categories, which overlap to some extend with the harms proposed by *Woods and Perrin*[1955]:

- Harms to personality rights, incl. protection of minors
  This category would cover, for example, defamation, hate speech, child pornography. The AVMSD would be one current EU law which could reference a duty of care standard that targets this harm. The problem here is that defamation is subject to national rules, which makes the creation of an overall standard problematic, if not impossible currently. One possibility could be to require Member States to incorporate reference to the duty of care standard in their local laws on defamation. This would likely preclude primary liability for this kind of harm because of the exclusive competency of Member States over substantive law in this area. However, as outlined above, primary lia-

1953 Pauline Westerman, 'Arguing About Goals: The Diminishing Scope of Legal Reasoning' (2010) 24 Argumentation 211, 212.

1954 Mark D Cole and Teresa Quintel, '"Is There Anybody out There?" – Retention of Communications Data. Analysis of the Status Quo in Light of the Jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR)' in Russell L Weaver, Jane Reichel and Steven I Friedland (eds), *Comparative perspectives on privacy in an Internet era* (Carolina Academic Press 2019) 81. Regulation 2016/679 (GDPR) Recital 173.

1955 Woods and Perrin (n 799) 35–41.

bility may not be a justified option in this field. It would also mean that explicit reference to the country-of-origin principle of such a duty of care would need to be made, although such a standard would likely harmonise substantive negligence based duties fully.

- Economic harms
  This covers mainly intellectual property rights, such as copyright and trademarks, but could also comprise online fraud. The substantive aspects of both IP rights are harmonised. It is perceivable that reference to this duty of care standard could also be inserted into IPRED, the Infosoc Directive and the DSMD.
- Harms to public security, order and democracy
  This category covers harms that threaten the stability of society, democracy, the environment or the functioning of the state. Terrorist content, the sale of prohibited products, such as trafficking in wildlife and protected species, weapons or drugs, are types of unlawful content that are contained in this section. The proposed TERREG could have a reference to a specific duty of care standard in this area. Other sector specific EU legislation would need to be identified that is suitable to carry references to this duty of care standard.[1956]
- Consumer protection
  This area covers, for example, products and services that are non-compliant, unsafe or prohibited. This area has a strong link to economic harms. Duty of care risk management considerations would likely be similar. In addition, they normally affect the same kind of platforms, such as online marketplaces or social media and messaging apps. A duty of care standard could be referenced in the recent MSR or in applicable *lex specialis* such as the Toys Safety Directive, and cross-referenced in the UCPD. This may entail classifying online marketplaces as economic operators under certain product safety *lex specialis*, but not in others.[1957] For food safety, the Official Controls regulation, the Hygiene of Foodstuffs regulation or the Food Labelling Regulation[1958] could be suitable places where such standards are referenced. Again, online platforms may need to be classified as food business operators

1956 Such as: Directive 2001/62. or the Directive 2008/99/EC on the protection of the environment through criminal law 2008 (OJ L 328) 99.

1957 This would depend on whether online platforms' business models potentially directly affect the essential requirements of these products. In that case the specific product safety standards (European Norms) could even contain obligations for online intermediaries.

1958 Regulation 2017/625; Regulation 852/2004; Regulation 1167/2011.

for this. It has been shown above, that food safety authorities could justify this classification where these intermediaries charge a commission or derive other revenue from the intermediation activity, i.e. through advertising.

The sectoral framework should also include specific protections for small or emerging platform operators. Such sandboxing requirements are known from other areas, such as financial regulation, where FinTech start-ups are given space to evolve and experiment without onerous compliance requirements at a crucial initial stage of development.[1959] Such requirements could, for example, be applied for the use of automated content recognition technologies or compliance with a technical, duty of care standard. The German *NetzDG* provides another example of how smaller platforms could be addressed. It frees social networks with less than two million domestic users from certain requirements relating to identification and removal of unlawful content.[1960]

4. The duty of care risk management system

At the heart of this proposal is a technical compliance framework in which platforms have to follow a risk-based approach in order to prevent and combat unlawful use of their systems. The division into prospective and retrospective duties of care is needed, because it is acknowledged that not all abusive uses of online platforms can be foreseen and pre-empted, even if prospective care was taken in an exemplary manner. Platforms launch new business models, algorithms and architectures on a frequent basis. They often experiment with new features or launch beta versions, which is part of agile software project management methods. This means that minor defects or lacking features may be fixed after launch. In this scenario, it is important that the intermediary has effective retrospective technologies in place that filter and monitor high risk activities and content areas, effective NTD procedures and other processes that involve stakeholders. This

1959 Dirk A Zetzsche and others, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 23 Fordham Journal of Corporate & Financial Law 31, 64–65; European Commission, 'Fintech: A More Competitive and Innovative European Financial Sector, Consultation Document' (European Commission 2017) 16–17 <https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf> accessed 9 January 2018.

1960 NetzDG para 1 (2).

would also be part of the continuous improvement that is part of a proper risk management approach.[1961] Prospective responsibilities relate therefore mainly to *ex-ante* measures that a platform should take in order to address harms that are reasonably foreseeable from its technology, architecture and business model. Retrospective measures would focus on *ex-post* measures that address unlawful content or activity as it occurs or happened in the past.[1962] Content filtering, which is often seen as a preventive measure, would, in its strictest sense be a retrospective measure.

The approach below seeks to mould risk management into a duty of care standard for online platforms by using the methodology laid out in the ISO 31000 risk management standard.[1963] This standard enjoys a wide applicability throughout the corporate world. It has been incorporated into other standards and is referenced in the EU risk assessment methodology.[1964] It is likely that most companies are familiar with its application, as well as with similar globally used 'societal' standards such as social responsibility (ISO 26000), anti-bribery management (ISO 37000),[1965] quality management (ISO 9001), or information security management (ISO 27001). A future duty of care standard could make us of this. In the following, the duty of care for online platforms will be broken down into the procedural steps of risk management (Risk identification, risk analysis and evaluation, and risk control). This is meant to demonstrate how a duty of care could be 'made concrete' within a platform business. For a broad concept like duty of care to work in an operational environment, it needs to be broken down into steps that can be directly applied to business planning, processes and systems. Such a lateral and structured approach will also give regulators and courts the means to verify whether the intermediary applied the required duty of care.

1961 Grant Purdy, 'ISO 31000:2009-Setting a New Standard for Risk Management: Perspective' (2010) 30 Risk Analysis 881, 883.

1962 Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (n 293) 48–49.

1963 'ISO - ISO 31000 — Risk Management' (*ISO*) <https://www.iso.org/iso-31000-risk-management.html> accessed 14 August 2020.

1964 European Commission, 'EU General Risk Assessment Methodology (Action 5 of Multi-Annual Action Plan for the Surveillance of Products in the EU (COM(2013)76))' (n 1945) 5. 'ISO - ISO/IEC 29100:2011(E) - Information Technology — Security Techniques — Privacy Framework' 18 <https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip> accessed 11 April 2020.

1965 Graz (n 1530) 47.

I. Risk assessment

According to standard methodology, risk assessment relies on three key steps: risk identification, risk analysis and risk evaluation. Analysis and evaluation are intricately linked and have been summarised under one section for simplicity here. An eventual technical standard would be expected to be more detailed and take account of various risk assessment techniques and formalities relating to the documentation and follow-up of risk assessments.[1966]

a. Risk identification

Risk identification will be done first in context of the particular statutory harms defined by law. This simplifies the process as the platforms will need to focus first and foremost on the public interests and fundamental rights. This does not mean that other risks should not also be picked up during the risk identification process. They may have knock-on effects on the wider risk environment the platforms operate in. For example, by considering the risk of counterfeit in the area of economic harms, an online marketplace or social messaging app may be able to identify additional risks related to money-laundering, product safety or fraud. Risk identification can be done in various ways. A platform could convene project and business teams on a regular basis, or engage in risk identification prior to the launch of major new features, such as a new content sharing feature, an algorithm update, or a new ad feature. As stated above, risk identification of platform design features, business models, architectures or algorithms is something that platforms will not always necessarily get right from the start. It lies in the entrepreneurial nature of many of these businesses that they launch new features or services, experiment with them and then decide whether to keep or discontinue them. This is why it is important that platforms have the procedural and organisational means in place to document these processes and review them regularly.

It is suggested here that an online intermediary first define clearly the most prominent (statutory) harms that may typically occur on their platform. They are expected to understand the wider risk environment in which they operate. This should be done by looking at internal data, escalations from outside users and other stakeholders and by consulting wider

1966 'ISO - ISO 31000 — Risk Management' (n 1962) para 5.4.

interdisciplinary research and feedback from society. This requirement could be adjusted to the size of the regulated entity. Certain platform models attract certain types of harms more than others. This should be documented when identifying risks of new design or business feature launched by the platform.

Secondly, online platforms should identify and understand the risk drivers related to their platform models. Risk drivers take account of the fact that the occurrence of unlawful content in itself is difficult to contain. However, platforms' architecture is capable of creating a framework that leads to an amplification of the risks related to the harms caused by unlawful content and behaviour.[1967]

For example, social media and UGC sites have been in the focus with regards to harms to personality rights and public security. Research in this area has shown that anonymity[1968] and nudging mechanisms for content propagation[1969] can be risk drivers for these harms. This does not mean that anonymity should be impossible. However, it should have consequences for the user and the way their content is (algorithmically) handled on the platform. In addition, adequate verification techniques should be in place. The way recommendation algorithms are structured and designed, the choice that is given to users to share or comment on content, or to whom it can be distributed, all influence the harms that can be caused.

For online marketplaces, typical risk drivers can relate to the provenance and legal status of sellers; or the type of product categories that the platforms offer to their sellers. This is also closely connected to anonymity or the ease with which a seller can start to sell on an online market platform. The sale of medicines, nutritional supplements or toys may pose a higher risk to consumers, and is generally regulated in a stricter way.

Following stakeholder dialogues a more complete example list of common risk drivers could be stablished for each harm and then incorporated

---

1967 Lavi (n 199) 54–56.

1968 David Babbs, 'New Year, New Internet? Why It's Time to Rethink Anonymity on Social Media' (*Inforrm's Blog*, 31 January 2020) <https://inforrm.org/2020/01/31/new-year-new-internet-why-its-time-to-rethink-anonymity-on-social-media-david-babbs/> accessed 14 August 2020; Kinsella (n 917). Jesse Fox, Carlos Cruz and Ji Young Lee, 'Perpetuating Online Sexism Offline: Anonymity, Interactivity, and the Effects of Sexist Hashtags on Social Media' (2015) 52 Computers in Human Behavior 436.

1969 Lavi (n 199) 18–35.

into a standard.[1970] This would necessitate empirical research and evidence gathering and broader stakeholder dialogues in order to get agreement of common risk drivers that impact harms on online platforms. This research is increasingly taking place,[1971] but the need to get even more data should be facilitated by obligations to allow independent researchers access to content data and propagation mechanisms on online platforms. The list of typical risk drivers can be continuously assessed and updated via regulatory guidance notes and eventual standard revisions. Platforms could brainstorm risk drivers before new business features are being launched or consult researchers, industry specialists or regulators on a confidential basis to help identify additional risk drivers.

b. Risk analysis and evaluation

Risk analysis means that each risk is examined in detail with regards to the impact of the harm caused and the likelihood of it occurring. Companies will need to have adequate and robust analytical capabilities and organisational structures in place that allow them to generate and apply internal data and intelligence for these purposes.

Platforms are also expected to understand the wider risk environment in which they operate, be it through participation in industry dialogues or by being in regular contact with regulators, researchers and user associations. It is obvious that, for example, periods of heightened terrorist risk or economic instability should be considered when platforms analyse risks that emanate from certain drivers. This can be supported through guidance and research from a regulator.[1972] This is also why many regulatory regimes require the existence of a structural nexus within a company, often in the form of a compliance function, in order to ensure specific regulatory risks

1970 This has been done in the next section's example case for online marketplaces, and in ANNEX III.

1971 See for example: Birgit Stark and Daniel Stegmann, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse' (Algorithm Watch 2020) .

1972 For example, the European Food Safety Authority (EFSA) or the European Agency for Health and Safety at Work (EU-OSHA) provide this analytical support on changing risk environments. 'Emerging Risks - Safety and Health at Work - EU-OSHA' <https://osha.europa.eu/en/emerging-risks> accessed 18 August 2020.

are being managed.[1973] In anti-money laundering law, regulated institutions need to appoint a compliance officer and, potentially, a specific internal audit function;[1974] the GDPR requires a data protection officer for certain entities.[1975] The duty of care regime for online intermediaries could require the establishment of a "safety officer" or another function that regulators can turn to for regulatory obligations, such as proof of risk assessments that the platform has to perform.

The risk analysis should lead to an evaluation and ranking of the risks by their seriousness. For example, if a new feature on a social media platform allows users to post or stream live video clips, then the platform would need to assess and evaluate whether this poses a serious, medium or low risk to: personality rights of privacy, personal integrity or harm to minors; economic harms related to copyright violations; public security harms related to terrorist content. It is also appropriate to ask platforms that allow users total anonymity to provide a risk assessment of specific harms. Again, a company would need to be able to have the analytical and organisational capacity to measure this risk. The sections on terrorist content, hate speech and copyright have shown that through initiatives like the GIFTC, or through NTD data, online platforms have the means to gather this information. It is submitted that even smaller platforms that are not part of industry initiatives or wider stakeholder groups should be able to capture and analyse escalations from users or regulators.[1976] Here, regulators in conjunction with industry associations, could provide support in helping these platforms in putting risk analysis and evaluation methods in place.

It is more difficult to verify the application of risk assessments when it comes to content management algorithms, especially where they rely on artificial intelligence. However, here too, the parameters and weightings that determine content decisions follow certain values and business objectives. A risk assessment would inevitably need to disclose these objectives as their impact on certain harms will need to be measured. Risk assessment could involve playing with these parameters to measure their impact on unlawful behaviour and content. Some methods how to address responsibility in this area have been mentioned in the previous section of this chapter.

1973 Griffith (n 1812) 2093–2095.
1974 Directive 2015/849 Article 8 (4).
1975 Regulation 2016/679 (GDPR) Section 4.
1976 This is supported by the fact that they have to be able to assess and react to notices of unlawful content or activity received by users.

Likewise, if an online marketplace were to launch a new product category, such as for example nutritional supplements, or allow sellers from a new geographic area to operate on their platform, then the economic risks to trademark rights or consumer protection risks to product safety could be assessed through different tools. First, a platform could look at the regulatory requirements of a new product area, such as (online) labelling, information requirements, risks to product integrity and the wider market environments (consumer and brand trends, counterfeit risks etc). It could then assess the risks related to letting unverified sellers from across the world list products in this area. It could also test the propensity of mistakes, such as incorrect labelling, or erroneous product information. After careful analysis it would then need to decide whether the activity or feature presents a high risk. As demonstrated in Chapter 3, courts in China have, for example, incorporated "red flag" (knowledge) tests into their duty of care regimes. A platform would automatically need to apply enhanced due diligence measures on content that is subject to high popularity or that goes viral, simply due to the size of the harm caused if that kind of content was indeed unlawful. In the area of copyright, the idea is that certain popular music or videos may be more susceptible to fraudulent practices.[1977] Likewise, viral content may create more opportunities for fraudsters. Chapter 4 has shown that red flags are also being used in predictive analysis by online platforms. A technical standard could provide indicative examples of typical red flags that would have to be considered in a risk assessment and evaluation.

A platform could also be required to score the risk of each legally defined harm when launching a new business, design feature or basic algorithms. Again, these mandatory risk assessments exist in other areas: the GDPR obliges data controllers whose activities pose a high risk to the privacy rights of individuals to perform a data protection impact assessment prior to starting their operations.[1978] Under anti-money laundering legislation, financial institutions need to identify and assess the risks of money laundering and terrorist financing;[1979] EU health and safety legislation[1980] requires that employers perform an assessment of the risks to safety and health at work. There are many more examples. The EU has provided am-

1977 Wang (n 504) 284–286.
1978 Regulation 2016/679 (GDPR) Article 35.
1979 Directive 2015/849 Article 8.
1980 Council Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work Article 9.

ple policy and procedural guidance to economic actors in these areas. Regulators could provide similar guidance and host best practice sharing and trainings to facilitate a consistent approach to risk assessment

II. Risk control measures

Risk controls are aimed at modifying the severity of a risk to an acceptable level. There are a number of possible risk responses that can be taken to address or control a risk. These shall not be covered in detail here.[1981] However, not all risk responses are appropriate to any type of risk. For example, risk assurance or risk sharing would not alleviate the harmful impact on users but just spread the punitive impact on the risk taker. In the context of the statutory harms and their risks discussed here, two risk responses would seem appropriate to address prospective responsibility: risk mitigation and risk avoidance. These responses would be broadly in line with the precautionary principle.[1982] If a platform was to launch a new feature or activity that it has classed as high risk with regards to certain harms then risk avoidance would see it refrain from deploying this feature or activity at least until it has brought in place proper safeguards. Bringing in place safeguards, such as user verification and restrictions on anonymity, or charging user fees, would in turn be counted as risk mitigation. In this case the platform would have taken a prospective responsibility to create a safer user environment.

Under its retrospective responsibility the platform would bring in place targeted monitoring and filtering, NTD or user flagging processes. These risk responses could be classed as contingency or fall-back measures because they deal with the risk once it materialises and becomes an actual harm. Although filtering systems do prevent unlawful content appearing on the site, this also means that a user was still able to access the site and (try to) upload this kind of content. Both prospective and retrospective measures should complement each other. An entirely prospective ap-

1981 For more detail see: 'ISO - ISO 31000 — Risk Management' (n 1962) s 5.5. Risk Treatment.

1982 Heidi Tworek, 'How Platforms Could Benefit from the Precautionary Principle' (*Centre for International Governance Innovation*, 19 November 2019) <https://www.cigionline.org/articles/how-platforms-could-benefit-precautionary-principle> accessed 17 August 2020. This author also suggests the risk assessment methodology as part of a precautionary principle approach for online platforms.

proach may throttle speech and content, while overreliance on retrospective measures may end up in frequent removals and sanctions without giving users an incentive to behave responsibly. Meanwhile, the ideal balance between both approaches may be different depending on the type of harm. It should be stressed that under this model, the risk identification and risk evaluation processes that feed into prospective and retrospective responsibility (control) measures are the same.

a. Risk control: prospective responsibility for empowering safe platform use

Prospective responsibility relies on the governance-by-design approach, which has become a wider policy approach with regards to technology driven businesses. This principle refers to "the purposeful effort to use technology to embed values."[1983] It has become prominent largely thanks to the endorsement by the GDPR's privacy-by-design approach. For the purposes targeted here, the principle imposed on platforms should be one of safety-by-design, by which platforms would need to embed online safety values into their services throughout the product development life cycle, including product updates.[1984] They do not just extend to architecture and processes but also to the way content moderation algorithms are designed by platforms, and the values and priorities they apply to suppression or amplification.[1985]

The platform would be required to address high risks related to statutory harms. As of now platforms have responded in a seemingly haphazard and reactive way to address high risk situations of certain harms by reacting to regulatory or public pressure. *Twitter* for example implemented a feature in August 2020 to give users more options over who can reply to their tweets. The measure is aimed at limiting trolls and the possibility of

1983 Mulligan and Bamberger (n 1777) 697. Florian Saurwein and others, 'Algorithmische Selektion im Internet: Risiken und Governance automatisierter Auswahlprozesse' [2017] kommunikation @ gesellschaft 22, 8.

1984 As suggested by: Woods, 'Duty of Care' (n 1703) 20–21. Woods and Perrin (n 799) 11–12, advocated, in principle, by: Helberger, Pierson and Poell (n 68) 6–8; Lavi (n 199) 19–30 and applied by: Great Britain and Department for Culture (n 197) 80–81.

1985 Gillespie, *Custodians of the Internet* (n 1010) 197–214.

hate speech and abusive comments.[1986] Other sites have started to impose enhanced user verification processes for participation, or consent mechanisms from other users when uploading images of them in a bid to ensure trust in more sensitive environments.[1987] Anonymity and user verification remain key design features that influence the riskiness of platforms and the content circulating on them. Linking different verification and anonymity levels to the way users can engage on a social media or UGC platform would be one way to control such risks.[1988]

Online marketplaces that integrate their own payments services will already need to ask sellers to undergo specific identity verification under existing anti-money laundering legislation. Additional risk control measures could foresee that sellers that want to sell in certain high-risk categories undergo additional due diligence or verification processes.

The 'best efforts' prescribed in the DSMD Article 17 (4)) relate to retrospective measures of filtering and NTD. They would be applied when the OCSSP failed to follow prospective duties of concluding licensing agreements with rightsowners for the content shared on its sites. Here, the additional question would be how an environment could be created that prospectively encourages users to refrain from sharing infringing content, where this poses a high-risk exposure to economic harms.

The AVMSD in Article 28b (3) also mentions possible prospective risk control measures that platforms may need to take in order to prevent unlawful hate speech or content that harms minors. These measures foresee technical features that allow users to report and flag content or implement parental controls.

Online platforms have ample mechanisms or risk control measures at their disposal to create user environments that allow for safe interaction. The exact detail of prospective (and retrospective measures) that are available, feasible and reasonable or proportionate for online platforms requires significant additional research and more formal discussions and negotiations between the various stakeholders. It is beyond the frame of this work to define the nature, scope and technical design of measures and processes for such a platform responsibility system. This would be at the heart of a safety-by-design standards creation process. Standardisation is a com-

1986 'Twitter Rolls out New Reply Controls to Combat Trolls' (*VentureBeat*, 11 August 2020) <https://venturebeat.com/2020/08/11/twitter-rolls-out-new-reply-controls-to-combat-trolls/> accessed 17 August 2020.

1987 Suzor (n 1223) 217–218.

1988 Babbs (n 1967).

plex and, unfortunately, lengthy process in which technical experts and other stakeholders from industry, technical bodies, the public sector, academia and civil society should engage. It normally takes several years before an initial standard emerges. However, once this onerous legwork is done, future updates and adaptions to changing technology and business realities can be done flexibly, while relying on established structures and resources.

For illustrative reasons, a non-exhaustive list of some important prospective design criteria shall be mentioned here. These rely on other research done in this area and on indicative case law where prospective or preventive duties have been endorsed by courts as part of reasonable due diligence measures. Some of these points have also been included in the example of a duty of care standard portrayed in the next section and described in more detail in ANNEX III.

- Anonymity management, user identification and verification measures (KYC)[1989]
  The effect of anonymity as a risk driver for unlawful behaviour has been described above in this section and in the sectoral analysis in Chapter 4. A platform would need to assess how much anonymous posting or uploading of content encourages the creation of harms. Some have suggested linking the degree of anonymity and user identification and/or verification by a platform to the kind of interactions the user is allowed to engage in.[1990] Minimum standards of identification or verification could be established in the duty of care standard, depending on the type and the severity of harms caused by anonymity and the fundamental rights affected. A scaled approach by type of harm appears to be also supported by case law. In *Delfi* the ECtHR underlined the importance of anonymity for freedom of expression in the context of user comments enabled on a news portal.[1991] In *Mc Fadden*,

1989 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 243–245. Niombo Lomba and Tatjana Evas, 'Digital Services Act - European Added Value Assessment' (European Parliament 2020) EPRS_STU(2020)654180_EN 283 <www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf> accessed 23 October 2020. Suzor (n 1223) 217–218.

1990 Anna Vamialis, 'Online Defamation: Confronting Anonymity' (2013) 21 International Journal of Law and Information Technology 31, 56–62. Babbs (n 1967).

1991 *Delfi* (n 777) paras 147–149.

the CJEU ruled that password protection of a publicly accessible Wi-Fi network, which resulted in a disclosure of the identity of the user to the network operator, was a proportionate measure to prevent harms caused by copyright infringements.[1992] In the area of e-commerce, even more onerous KYC and identification processes may be adequate due to the potential harm of counterfeiting to a combination of consumer safety, economic interests and financial transactions. The latter may already require platforms to apply enhanced identity verification of sellers under EU anti-money laundering legislation where they offer payments services.[1993] Similar provisions exist in the area of food safety, which requires online sellers of food products to register their activity with national food safety authorities. Online intermediaries that facilitate the sale of food products by third parties could be obliged to verify this registration with sellers before allowing them to sell on their platforms.

Solid processes for user identification may create a trustful environment simply because of their deterrent effect to abusive users, but also because they enable a better administration of retrospective measures, such as sanction processes. In this context, *Zeno-Zencovich* argues that anonymity rules on the internet can and should be adapted to who communicates, what, where, with whom and how, and the competing interests at stake.[1994] Concerning the who, individuals, groups of individuals and business entities could be given differentiated anonymity options,[1995] or verification procedures. Regarding the 'with whom', the circle of addressees (public/defined groups/individual) could trigger different anonymity requirements, depending, for example, on the speech context, the frequency of engagement, or the interests and rights at stake.[1996] This typology could provide a useful base for risk controls that finetune anonymity with the aim of mitigating harms. This leads to the next point.

1992 *Mc Fadden* (n 139) para 96.
1993 Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet' (n 747) 239–240. Directive 2015/849 Articles 13 - 18.
1994 Vincenzo Zeno-Zencovich, 'Anonymous Speech on the Internet' in András Koltay (ed), *Media Freedom and Regulation in the New Media World* (Wolters Kluwer Kft 2014) 107.
1995 ibid 107–109.
1996 ibid 110–113.

- Providing benign user engagement options (in reply, sharing, creation, commenting or flagging content);
  As noted at various points in this work and by many other commentators, content moderation on digital platforms is steered by economic interest. This also determines the choice that users have in their interactions with each other and with content. More benign interaction opportunities would, however, limit or abolish those architectures or technical features that cause or amplify harm.[1997] The recent example of *Twitter* (see above), by which users are given more options in determining who can reply to their posts is one example that appears to follow the line of argument developed by *Zeno-Zencovich* above. Another solution could be to define and bolster the roles of independent, institutional trusted flaggers or community managers from civil society, regulators or other institutions. They could intervene preventively in certain harms, not only by flagging content but also by plugging their own software into platforms' APIs in order to identify, monitor and evaluate harmful content and behaviour.[1998] *Woods and Perrin* suggest that for certain contexts user interaction could be deliberately slowed down. This could be done to motivate users to engage more thoroughly with some contents before simply reposting them.[1999] It would eventually be the work of the standardisation process to evaluate and consolidate the ample research that is currently going on in this area and define some key mechanisms and tools as state of the art against the use of which platforms' duty of care would be measured.

- Allowing for computational reproducibility and independent assessment of content management and filtering algorithms[2000]
  Given the opacity and complexity of content moderation and the continuation of unlawful content, this transparency requirement is a crucial first step towards for creating the independent oversight needed to control harms.[2001] The duty of care and responsibility of platforms should therefore, at least during an initial phase, be measured by how

1997 Lavi (n 199) 26, who calls these feature 'evils nudges'.
1998 Gillespie, *Custodians of the Internet* (n 1010) 125–136.
1999 Woods and Perrin (n 799) 14–15.
2000 Mulligan and Bamberger (n 1777) 782.
2001 Gillespie, *Custodians of the Internet* (n 1010) 198–199; Gorwa, Binns and Katzenbach (n 1066) 10–11; Karen Yeung, 'Why Worry about Decision-Making by Machine?' in Karen Yeung and Martin Lodge, *Algorithmic regulation* (2019) 28.

transparent platforms are in providing the data behind harms. This could include obligations written down in the standard on: providing researchers and regulators access to databases and algorithms, e.g. through APIs and testing interfaces that allow for simulation or replication of content moderation processes;[2002] providing information on the data used to train algorithms; disclosing the parameters and methodologies that influence algorithms; detail about the human involvement in decision-making; an account and explanation of the updates made to content management and filtering algorithms.[2003] All these requirements could follow or draw on current and emerging open standards and mechanisms for the accountability of algorithmic and AI systems, that are more transparent than voluntary self-regulatory codes.[2004]

- Content management algorithms that incorporate considerations of harms and fundamental rights;
  Research on this issue has been gathering in breadth and depth.[2005] The principles that should underpin architectures and algorithms practices will likely need to follow broad ethics principles. The normative objectives of such impact assessments could be tied to principles set down in sectoral legislation. An example is provided in the sample duty of care standard in ANNEX III. Similar to requirements in the GDPR, platforms could be required to perform harms impact assessments of their systems for harms that pose high risks. Platforms would need to disclose these assessments to regulators and report on the use of the measures from the toolboxes described in the previous bullet points to address these harms. Multidisciplinary expert teams[2006] assembled by regulators, including for example engineers, psychologists, sociologists and lawyers would be required to review the risk control measures pro-

2002 Perel and Elkin-Koren (n 1918); Mulligan and Bamberger (n 1777) 253.

2003 Mulligan and Bamberger (n 1777) 781; Ioanna Miliou and Dino Pedreschi, 'Artificial Intelligence (AI): New Developments and Innovations Applied to e Commerce.' (European Parliament 2020) 13–14 <https://data.europa.eu/doi/10.2861/2605> accessed 27 October 2020.

2004 Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (n 293) 67–69. Brown and Kennedy (n 1883) 357–361.

2005 Yeung and Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (n 293) 68–72. *Andrews* provides a useful typology of algorithmic harms that pose challenges for public policy. Andrews (n 1777) 210–211.

2006 Gillespie (n 1010) 198.

posed by platforms. All this assumes, that achieving and maintaining fair content management and platform systems is an ongoing process, whose intensity will depend on the measurable presence and impact of harms.

Transparency on the design and use of algorithmic content management and filtering systems, even where the latter are part of retrospective responsibility measures, are a distinct feature of a prospective responsibility. Transparency signals a commitment on the part of a platform to be scrutinised by stakeholders and to be open to improvements and adjustments when it comes to managing harms. It therefore promotes a wider culture of cooperative responsibility. However, transparency should not only apply to complex algorithmic and architectural decisions. More straightforward aspects, such as simple and easily accessible terms and conditions on e.g. prohibited content and behaviour, and the possible sanction mechanisms will also go a long way to creating a culture of trust and safety.

Some commentators have argued that in order for a substantial shift to happen, the underlying business rationale of today's digital platforms needs to be changed. *Gillespie* argues that, if the revenue basis were to move away from advertising (maximised through excessive user attention grabbing), complementary regulatory tools may be needed. Competition, data protection and consumer protection tools such as data portability, interoperability, transparency and a right to an explanation may steer the industry towards subscription based systems that value more long–term and equitable user interaction.

b. Risk control: retrospective responsibility to contain unlawful content

Although retrospective responsibility is more difficult to be attributed to actors that are not the originators of unlawful information and harm caused, the previous sections have shown that failure to take on prospective responsibilities also facilitates the occurrence of harm. Therefore, there is a link between prospective and retrospective responsibilities in deontological argumentation.[2007] In addition, there are clear consequentialist reasons,[2008] e.g. the cheapest cost avoider argument, that justify retrospective responsibility.

However, were prospective safety-by-design principles applied in a perfect way, there would be no need for retrospective risk management. That perfect situation is unlikely to happen. First, uncertainty is one characteristic of risk, and not all risks can always be adequately predicted and evaluated. The particular nature of technology, project and software management means that some risks may only appear during or after launch of a new business feature. Some risks may have been simply misjudged or the controls were not adequate.

Secondly, low or medium risks may become high risks, for example when regulation, technology or user habits change, or seemingly unrelated factors impact on online platform ecosystems.

Lastly, depending on the type of harm, prospective responsibilities may be more difficult to take on. In the area of copyright, it may be more difficult to steer responsible behaviour if a UGC platform is unable to gain authorisations from rightsowners. Other prospective risk control measures do not appear to be realistic given the complexity of limitations and exemptions in copyright. For example, user verification measures would do little in discouraging a user from uploading infringing content if they are not aware of the licenses the platform holds or if they are unaware of the intricacies of copyright. Therefore, the best efforts stipulated in Article 17 (4) of the DSMD focuses more extensively on retrospective measures of content filtering and NTD.

Retrospective measures in the context discussed here are aimed at limiting the impact of unlawful content or activity. Content monitoring and filtering, enhanced control measures for red flag events, NTD processes, as well as effective sanction policies and procedures would be the most common retrospective responsibility measures.

2007 Vedder (n 292) 73.
2008 ibid.

Retrospective risk control measures should focus on instances of high-risk content and behaviour where they occur on the platform. Apart from that, they would also serve to monitor and measure the efficacy of prospective tools. For example, high risks to consumer protection harms emanating from the launch of a category of new sellers or products on a marketplace could be addressed by advanced due diligence during seller onboarding and *ex ante* product verification requirements. However, the platform would still put in place retrospective measures of enhanced transaction and listings monitoring in order to measure the impact of the prospective measures and spot potential gaps in the process. Once the risk is classed as medium or low, it would still continue monitoring, albeit on a less intensive basis. This continuous monitoring of the risk environment through retrospective measures also helps to stay alert of any changes in the risk environment. This should also be included as a requirement in a duty of care standard. This kind of approach is also used in other areas. Under anti-money laundering legislation, financial institutions have to have prospective measures of due diligence in place for lower and high risk clients. At the same time, they also need to have systems in place to identify potentially unlawful behaviour, for example through monitoring for suspicious transactions and behaviour according to established criteria.[2009]

III. Example of a duty of care standard for economic harms

ANNEX III provides a possible approach and format of a risk-based duty of care standard. This standard was developed in 2019 together with *React*, a global anti-counterfeiting industry association, based in Amsterdam. A fact-finding exercise conducted by *React* as part of this project in autumn 2018[2010] revealed a wide variety of different policies, processes and capabilities of online marketplaces globally, but also within Europe, when it came to fighting and preventing counterfeit products. For example, within Europe the survey found that the reaction to notices varied significantly between marketplaces. While many operators responded within one to three

2009 Directive 2015/849 Articles 13 (1) (d), 15 (3), 18 (2).

2010 REACT had contacted 11 nationally operating European marketplaces (of which one in Russia), one regional operator based in South America, 22 Asian marketplaces, of which nine were operating internationally, and seven North American based marketplaces, of which five operated globally. This survey is not included in the duty of care standard document of ANNEX III.

days to notices, some could take up to one or two weeks to action these requests. A majority did not have any counterclaims processes in place nor did they state any service level agreements (SLAs) to notice filers. This disparate picture was mirrored on a global level. This is of relevance since a number of these operators, while not having any subsidiary in the EU, may still target EU consumers. The majority of European marketplaces contacted appeared to have no solid sanctioning or suspension processes in place against infringing sellers. Consequently, the re-appearance of previously notified and removed products and sellers remained an endemic problem on all but one platform contacted. This was also a problem in many of the marketplaces contacted outside of Europe, including large, global players. None of the marketplaces contacted by *React* in Europe had any transparency reports about their NTD activity, counterclaims or sanction processes in place. A minority engaged in more proactive communication and education of sellers regarding the compliance requirements with regards to IP rights on the platform. None of the platforms contacted in Europe confirmed the existence of voluntary proactive measures to identify and prevent counterfeits. In North America, only one player had such processes in place, while in Asia the large majority of platforms contacted had voluntary proactive measures in place. This may reflect the more hawkish stance of courts and legislation on intermediary liability in countries like China or India mentioned in Chapter 3. However, the actual detail of these proactive measures remains unclear. In Europe, four of the 11 marketplaces contacted had a dedicated IP program in place that allowed brand owners expedited access when it came to identifying and notifying trademark violations. In North America, the majority of platforms had such programs in place, while in Asia seven out of the 22 marketplaces contacted offered this service to brand owners.

Taking these disparate situations as a departing point, the project undertook to define standard processes and capabilities that e-commerce platforms should have in place in order to identify and address the highest risks of counterfeit and the sale of unsafe and illegal products. The aim of this exercise was to establish common, reasonable measures that can be expected from online marketplaces worldwide when it comes to acting responsibly towards the risk of counterfeit and non-compliant products. For one, this solution aims to establish a platform responsibility level that is higher, and according to this opinion, more adequate, than the current minimum requirements in EU (and US) legislation. Secondly, this unified approach would level expectations of all platform stakeholders and provide better predictability, transparency and accountability. Thirdly, the

standard approach provides also for flexibility, as it is an adaptable system. In addition, the risk management process itself allows platforms to respond to risk drivers that are specific to their business model.

It should be noted that this exercise did not take any existing legislation in Europe or elsewhere as a limiting reference. It has been shown in Chapters 3 and 4 that the current liability exemptions framework in the EU (and elsewhere) limits the mandatory actions that platforms need to take to combat unlawful content and products to mere reactive duties and a tightly circumscribed set of proactive obligations. In reality, however, most platforms, even smaller ones, have today access to substantial data and can exert a certain degree of control over offers and advertisements on their systems. Data and fees generated from online transactions and advertisements generate the bulk of their revenue. In addition, platforms increasingly integrate a number of other remunerated services. They may offer payment transactions and related services, logistics, promotional or optimisation services.[2011]

Based on these considerations, the proposed duty of care standard in ANNEX III assembles the most common features of online marketplaces today and sketches out a risk management approach that platforms could reasonably be expected to apply when conducting their business. The system is centred on the recognition and management of two types of harms that may be facilitated by e-commerce marketplaces today: 1) economic harms related to the offer of products and advertisements that constitute trademark violations, and 2) harms to the public interest of consumer protection caused by the sale of unlawful (unsafe, non-compliant, illegal) products.

The standard incorporates principles of existing common risk management systems that are widely applied throughout the corporate world and that may already be familiar to platforms and their stakeholders: ISO 31000:2009 Risk Management, ISO 29100:2011 Information Technology – Security Techniques – Privacy Framework, ISO 20488:2018 Online consumer reviews. Following a risk management approach, the standard identifies common risk drivers related to three larger categories from which harms may be caused: sellers, product (categories) and the platform's business model (e.g. architectural design, service integration). The standard provides more detailed operational risk drivers relating to each category. A

2011 The proposal also draws on the professional experience of the author as a fraud detection, compliance and audit manager at a global online marketplace and retailer.

(future) standard could specify that, at a minimum, some or all of these drivers must be covered in a risk assessment exercise, or alternatively, leave this list as an entirely indicative and non-exhaustive guidance.

As part of the risk assessment, the drivers would need to be analysed and quantified. Online marketplaces would need to have capabilities and resources in place in order to conduct such a risk analysis. A number of these organisational and structural pre-requirements have been provided as part of the standard. It is clear that smaller players may not have the same capabilities as larger players. However, the proposal suggests that a minimal risk analysis based on internal data and awareness of the external risk environment should be imposed on all platforms. This ties into the argument that the actual knowledge standard is not any longer adequate as a liability standard for current online marketplaces, or any of the online platform business models covered here. The voluntary choice to engage in (Web 2.0.) platform business models requires a parallel build-up of knowledge and risk assessment methods to address potential harms. Actual knowledge of unlawful acts is a reactive concept that does not befit today's online platforms. It needs to be supplanted by an approach whereby the platform is required to become knowledgeable and aware of the risks of its business. An online marketplace needs to have tools and structures in place that help it deal with uncertainty, by establishing the potential impact of the harm caused by certain risk drivers and the likelihood of them occurring through its platform (the core of the risk assessment). These capabilities can also be relied on when establishing transparency and reporting obligations for these actors. Example of such internal tools would be the capability to capture and analyse notice and takedown data, the establishment and analysis of seller sanctions, or internal (documented) brainstorming and review processes when launching new platform features or services. This could tie in with the methodology of established ISO standards and industry practices. External capabilities would consist of the integration of brand owner or industry intelligence. Where an online marketplace qualifies as a trader, this could link in with the standards of professional diligence referred to in the UCPD.[2012]

The capabilities will be essential for measuring and rating the risks of the harms that emanate from the risk drivers. The risk rating procedure would need to be documented internally, with a potential obligation to conducting it in regular intervals or every time a significant change hap-

2012 Directive 2005/29/EC Article 5 (2) (a), Recital 20; European Commission, 'UCP Directive Guidance' (n 57) 123–132.

pens in one of the broader risk driver categories. Regulators could be given powers to consult these procedures on request. The platform would need to put measures in place to address identified high risks. The proposed standard lists a number of such measures. They correspond to both the prospective and retrospective duties discussed in this chapter. For example, high risks relating to certain product categories or seller profiles would necessitate enhanced onboarding or verification procedures prior to these products or sellers going live on the platform. Retrospective measure would include enhanced monitoring of transactions in specific, high risk product categories or for specific, high risk (gropus of) sellers. A non-exhaustive list of control measures for high risks is given in the standard in ANNEX III. The management of high risks necessitates enhanced analytical, organisational and structural capabilities on the side of the platform.

The standard also proposes procedural requirements for NTD on online marketplaces. The disparate nature of NTD processes was one of the problematic areas identified in the survey conducted by *React*. Unified standards will go a long way in establishing a level playing field across platforms and producing procedural transparency and predictability for the various platform stakeholders.

Finally, the standard suggests measures that aim to instil more transparency into the content management activities of online marketplaces. Some of these, like the requirements to provide clear terms and conditions and actions taken *vis-à-vis* stakeholders that violate platform policies, would feed into prospective responsibility measures. On the other hand, transparency reporting obligations, possibly separated into publicly accessible reports and into confidential reports for regulators or defined stakeholder groups, aim at helping to fill the accountability and transparency gaps that have been a central criticism against platforms. Secondly, these reporting requirements may also help platforms to identify the capacities needed to detect, measure and control high risks.

5. Transparency and accountability obligations

I. Transparency

The need for platforms to be more transparent about almost everything that negatively affects users has been repeated by many commentators and

for many years.[2013] Transparency in the way information is managed on platforms would be essential in order to understand how and why, for example, unlawful content is spread and remains accessible. This does not require complex disclosure statements or technical reports, which may be protected by trade secrets of companies or are simply not intelligible for the average user.[2014] Alternative solutions are live visualisations and explanations of *why* certain content pieces are repeated or exposed. *Gillespie* argues that platforms could empower users and civil society associations to identify abusive and unlawful content, which would directly help other users to make decisions on whether they want to access this kind of content.[2015] A co-regulatory standard could list such prospective transparency systems that allow users to create safe and responsible online platform spaces.

Secondly, there should be minimum standards of transparency when it comes to automated content filtering systems.[2016] Again, the detail required may differ when looking at the target audience. But given the high degree of automation in content filtering and takedowns, more transparency goes a long way in addressing how platforms act responsibly and consider all stakeholders' interests and rights. As of today, some platforms have given a certain degree of insight into their moderation processes and decision criteria. But this varies by area. In the areas of hate speech and copyright some transparency reporting has been put in place by platforms. However, concerning terrorist speech, counterfeiting, defamation or unsafe products there are virtually no detailed reports available. In addition, details on the accuracy of removal decisions, appeals processes and detailed management of take down decisions remain widely inaccessible. In effect, these systems remain out-of-control systems, that are highly automated and opaque.[2017] This throws into the dark the risk management procedures that have been applied by these platforms. It is not clear, for example, whether automated systems favour commercial over legal criteria, which is an allegation made frequently and which goes against a responsible duty of

2013 Gillespie, *Custodians of the Internet* (n 1010) 198–199; Citron (n 914) 31; OECD, 'The Economic and Social Role of Internet Intermediaries - DSTI/ICCP(2009)9/FINAL' (n 46) 10–12, 88. Bamberger (n 37) 727–730.

2014 Yeung (n 2000) 28.

2015 Gillespie, *Custodians of the Internet* (n 1010) 199–200.

2016 Gorwa, Binns and Katzenbach (n 1066) 11.

2017 Christian Katzenbach and Lena Ulbricht, 'Algorithmic Governance' [2019] Internet Policy Review 10–11 <http://policyreview.info/node/1424> accessed 28 January 2020.

care approach.[2018] The current obligations of transparency reports in national legislation, such as in the German *NetzDG* are a good start but they do not go far enough. The main idea is that, far from just throwing data at the public that is sorted in a way that appears to give meaningful information, regulators need to come up with requirements that expose the risk assessments and control measures for each harm and that show how fundamental rights have been respected in this process. The way in which humans are being involved during automated content-decision-making, harmonised metrics on decision accuracy, the number of appeals and content reinstatements, should be publicly accessible. Meanwhile, regulators should have insight into the detailed design parameters that determine control measures. The regulator should still require platforms to report on a regular basis on the operation of their NTD systems. NTD systems are still a crucial retrospective responsibility measure for smaller platforms.[2019]

II. Accountability

Transparency on its own is of limited use. But it is a means to hold internet intermediaries accountable for the content management decisions they are taking on a daily basis and that *de facto* regulate our information access to the internet today. Since the 1980s, there has been an accelerating trend in software development of relying on empirical techniques to the detriment of theory and systemic reasoning. According to *Clarke and Wigan*, big data, machine learning and algorithmic decision-making represent the current pinnacle of systems that do not need to be logically justified any longer, in contrast to earlier principles of software development.[2020] Online platforms of today are the embodiment of such empiricism. This initially naïve and now fervent application of computing power has led to a lack of ethical responsibility for harm caused by decisions delegated to machines;[2021] it has by now become high-jacked by purely commercial motivations.

2018 Sylvain (n 795) 59; Pasquale (n 19) 496; Damian Tambini, 'Social Media Power and Election Legitimacy' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 289.

2019 Urban, Karaganis and Schofield (n 661) 59.

2020 Clarke and Wigan (n 84) 693–694.

2021 ibid 694.

Transparency will help regulators and civil society to ask online platforms the right questions about the ethical parameters, focussed on harm, that have or have not gone into content management and platform design decisions. The focus on transparency would aim to reinstall procedural accountability.[2022] That procedural accountability will be structured through the duty of care risk management standard. That standard provides a guideline of how the ethical values – embodied by the harms and fundamental rights that need to be balanced – are being incorporated into platform design and content management. For example, the privacy-by-design standard pursued in the GDPR has been explicitly endorsed as an appropriate means to achieve accountability for compliance of operational procedures with data protection principles and values.[2023] The eventual measurement of the effectiveness of the duty of care standard would be part of a more outcomes-based accountability.[2024] This would be achieved through regular transparency reporting, independent stakeholder dialogues and reports and assessments by the regulator.

III. Complementary regulatory approaches towards online platforms

It has been argued by a wider circle of commentators that an online intermediary responsibility framework would be most effective if supplemented by more holistic regulatory initiatives in other contentious area of digital platform power.[2025] While the delimitations offered in the introduction have made clear that neighbouring substantive law areas that affect the digital platform economy cannot be treated here, a brief overview of these complementary measures shall still be given.

Some key regulatory advances have been made recently in neighbouring areas of intermediary responsibility. The GDPR gives data subjects new

2022 Bunting (n 66) 21–22.

2023 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor' paras 101–117 <https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en> accessed 19 August 2020.

2024 Bunting (n 66) 22.

2025 Pasquale (n 19) 489; Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661). Damian Tambini, 'Platform Dominance' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 62–63.

and enhanced rights. It allows for data portability, the right to object to and obtain an explanation on fully automated decision-making procedures, including profiling, and to rectification and erasure of personal data.[2026] Meanwhile the privacy-by-design principle and the data protection impact assessments impose more procedural and architectural responsibilities on data controllers (and processors). Because user and content data (exemplified by 'big data') have moved to the heart of the business model of most online platforms today, the GDPR may be one tool to curtail the unchecked collection and processing of user data. It is still too early to tell what influence the GDPR will have on the activities of online platforms. Experts are, however, divided.[2027] Some estimate that the GDPR may well help break the monopolistic tendencies of digital platforms. A stronger move towards subscription-based business models may well help address the anonymity challenge and break some of the more vicious nudging practices.[2028] Others, however, are less optimistic and see that the GDPR does not provide adequate tools to address the reality of the current pervasive data gathering and processing practices on digital platforms. It may even be wishful thinking.[2029]

The 2019 Omnibus Directive strengthens the positions of consumers *vis-à-vis* online marketplaces by imposing stronger transparency requirements on the latter. It adds to the trend of defining platform business models and establishing specific responsibilities for these actors. The AVMSD and the DSMD have already introduced definitions for VSPs and OCSSPs. The Omnibus Directive does the same for online marketplaces.[2030] This definition, updated from previous EU Acts, clearly classifies these actors as traders under the UCPD and confers professional due diligence obliga-

2026 Regulation 2016/679 (GDPR) Articles 16 - 22.

2027 Shoshana Zuboff, '"We Make Them Dance": Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) 33–34 <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020.

2028 Edwards, 'With Great Power Comes Great Responsibility?: The Rise of Platform Liability' (n 661) 289.

2029 Joris van Hoboken, 'The Privacy Disconnect' in Rikke Frank Jørgensen (ed), *Human Rights in the Age of Platforms* (The MIT Press 2019) <https://direct.mit.edu/books/book/4531/Human-Rights-in-the-Age-of-Platforms> accessed 28 May 2020; Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data.' (2017) 47 Seton Hall Law Review 995, 1003.

2030 Omnibus Directive 2019/2161 (n 1249) Article 3.

tions on them.[2031] Online marketplaces will need to disclose the parameters that influence search rankings to consumers and also call out any rankings that are influenced by advertisements.[2032] They also have to provide clear information regarding the legal status of third parties that are offering goods and services on their platform.

In a similar vein, the Platform to Business (P2B) regulation obliges platforms to disclose ranking parameters behind search results to business users, and disclose where and why differentiated treatment exists that may bias the display of search results.[2033] This regulation is in itself a valuable testimony to the fact that online search intermediaries do determine how content is displayed to users and that this is influenced by commercial priorities. This questions yet again the active/neutral dichotomy of the current liability regime. Any lessons drawn from the disclosure of ranking and differentiated treatment parameters may, arguably, be important when drawing up transparency obligations for other content management practices under a new online platform responsibility framework. Under both the P2B Regulation and the Omnibus Directive search intermediaries are, understandably, not required to disclose publicly the detailed functioning of their ranking mechanisms and the algorithms behind it.[2034] However, experience from the operation of these requirements may still help to gauge a possible requirement to disclose public interest and fundamental rights criteria of content management algorithms under a duty of care standard for online platforms.

6. The regulatory institution

Chapter 4 has demonstrated that the commonalities of the technological operations, legal challenges with content and responsibilities, and the convergence of content specific laws call for an overarching, principles-based

2031 Directive 2005/29/EC 29 Article 5.

2032 Omnibus Directive 2019/2161 (n 1249 Article 3. This follows initiatives taken at Member State level, such as in France – see: Élise Poillot, Natacha Sauphanor-Brouillaud and Hélène Aubry, 'Droit de la consommation' [2018] Recueil Dalloz 583.

2033 Platform-to-business (P2B) Regulation 2019/1150 (n 1248) Articles 5, 7; Omnibus Directive 2019/2161 (n 1249) Recital 23.

2034 Omnibus Directive 2019/2161 (n 1249) Recital 27.

approach. This is supported by various other commentators.[2035] Given the influence of online intermediary regulation on the internal market's free movement principles and its impact on fundamental rights it would appear appropriate to create regulatory powers that are, at a minimum, strongly coordinated at EU level by Member States and their competent regulatory authorities. The AVMSD has already allocated some responsibilities in this matter to the European Regulators Group for Audiovisual Media Services (ERGA), which exists since 2014. However, ERGA currently acts simply as an advisory body, representing Member States' national regulatory authorities for audiovisual media services. France had broadened the powers of the *CSA* for intermediary regulation in several areas. *Woods and Perrin*[2036] have argued for the UK that a horizontally focussed regulatory institution that takes on issues of platform responsibilities would be an adequate way forward. Since this work proposes a co-regulatory approach, it does support the view that a more enhanced degree of regulatory supervision than is currently the case is necessary. Given the need for managing society stakeholder dialogues, conducting additional research, overseeing the creation, supervision and auditing of compliance with and the effectiveness of a new technical standard for duty of care, a broad regulatory mandate will be needed. The new regulatory institution, whatever form it may take, will need to recruit technical and research expertise, policy capacities, as well as judicial competences. With the immense gaps in governance readiness that exist today in this area[2037] the new institution could become an important building block towards supporting and coordinating the construction of the necessary regulatory capacities in policymaking and in enforcement. Further intense policy dialogue and research would be needed to establish the status of such a new regulatory setup.

One option could consist of a council or other body of national regulators and agencies that is supported by a scientific agency on the lines of the European Food Safety Authority (EFSA) or the EU Agency for Safety and Health at Work (EU-OSHA). The EU's current Observatory on the Online Platform Economy could, for example, be the nucleus for such an institution. Alternatively, a more centralised, broad and powerful regulatory authority on the lines of the European Banking Authority (EBA) could be an-

2035 Lipton (n 23) 155-157; Taddeo and Floridi (n 120) 1598; Burk (n 295) 452; Valcke, Graef and Clifford (n 1653) 710–711.
2036 Woods and Perrin (n 799) 55–57.
2037 Andrews (n 1777); Freeman (n 1777) 79–81. Cohen (n 19) 383–397.

other option. The creation of a strong regulator with more epistemic authority may, however, go against the demands of responsive and flexible regulation that maybe more appropriate in the area of platform responsibility.

Given the complex, multi-layered and vertical structures of content law regimes and the need for a strong horizontal framework of overarching principles and responsibilities, a looser structure could be more effective. The complex regulatory structures outlined in Chapter 4 reflect the distribution of competencies under the various legal and content areas between the EU and Member States. Any overly centralised solution is likely to bring to the fore the (substantial) overlap and conflict of competencies that exist when regulating platform responsibility relating to unlawful content. It would include aspects as diverse as media policy, product regulation, personality rights, property rights, public security and consumer protection. It is outside the frame of this work to engage in further analysis of the most appropriate regulatory setup to regulate platform responsibility. To give just one example, however, *Kerber and Wendel et al* have shown that in the area of telecoms regulation, the EU relies on a regulatory network that is held together by a central body (BEREC) with specific tasks and powers. Despite the retention of competencies by national telecoms regulators, BEREC initiated the vast majority of regulatory activity, such as issuing guidance notes, reports or setting standards.[2038] Because of its decision-making structure, its specialist working groups and its influence in conflict resolution, it has become a key governance instrument that impacts rule-making in this area.[2039]

Any solution would most likely be the result of intense political compromise between Member States and the European Commission. More detailed suggestions and possible avenues, that take on board the challenges of enforcing new responsibility provisions in the context of the diversity of content on platforms today, are being currently explored. All of these acknowledge the cross-border challenge of the issues and call for enhanced regulatory cooperation at EU level.[2040] This could provide a basis for further research.

2038 Kerber and Wendel (n 1810) 10–13.

2039 ibid 12.

2040 Cole, Etteldorf and Ullrich (2020) (n 17) 45–48, 258–261; 'ERGA Position Paper on the Digital Services Act' (European Regulators Group for Audiovisual Media Services (ERGA) 2020) <https://erga-online.eu/?page_id=14> accessed 5 November 2020.

7. Brief of evaluation of the Commission's DSA proposal of December 2020

As stated in the introduction, the completion of this work coincided with the European Commission's own, long awaited publication of its proposal to adapt the responsibilities of online intermediaries. A brief analysis that focusses on main common points and differences from the solution proposed here shall therefore be appropriate.[2041]

The Commission chose to treat the question of liability exemptions and that of additional responsibilities as separate issues. That structure, however, is implicitly self-imposed by the Commission's choice to transplant the current ECD intermediary liability exemptions regime almost unchanged into the new DSA. The retention of controversial concepts of neutrality, actual knowledge, expeditious removal and the addition of a "Good Samaritan" provision are unlikely to provide for more clarity for courts and legislators in the future, as the intermediary landscape evolves. This is despite the clarifications, derived from EU case law, that Recitals 18 and 22 of the DSA proposal are supposed to provide on the neutrality and the actual knowledge conditions. In addition, the DSA proposal, predictively, keeps the prohibition of general monitoring due to its significance for fundamental rights protection. However, whether Recital 28, which states that general monitoring does not mean monitoring obligations in specific cases, provides the clarification that was widely demanded on this issue, is doubtful.[2042] Meanwhile, the scope of the liability exemption has been narrowed by obliging intermediaries to comply with illegal content removal and information disclosure orders. While the unchanged insistence on the intermediary liability exemptions can be seen as somewhat surprising, given the persistent criticism of its design, the issue is relegated to second stage by the imposition of free-standing, due diligence obligations. These due diligence obligations would apply regardless over whether or not an intermediary qualifies for the exemption conditions outlined in Articles 3 – 9 of the proposal and regardless of whether and what kind of liabilities it would incur under national rules. The Commission decided against exclusive, free-standing positive obligations, as advocated in this work, due to

2041 For a more detailed analysis see: Cole, Etteldorf and Ullrich (2021) (n 548).
2042 ibid 139-140 (81–82).

doubts over a potential conflict with the proportionality and subsidiarity principles of such a solution.[2043]

The creation of harmonised positive due diligence obligations, on the other hand, are to be welcomed. Again, this is not the place for an in-depth analysis. The DSA proposes staggered obligations that increase with the degree of involvement of the intermediary in the intermediation processes and its potential to create harm.[2044] The due diligence obligations accumulate successively, starting from intermediaries at the lowest level (Articles 10 – 13), all hosting providers (Articles 14 – 15), online platforms (Articles 16 – 24) and, finally, very large online platforms (VLOPs) (Articles 25 – 33). Similar to the proposal put forward in this work, the DSA aims to set these obligations at a horizontal level and without prejudice, or as complimentary provisions, to existing or future sectoral provisions. The AVMSD, the proposed TERREG, the Regulation on the marketing and use of explosives precursors, the P2B Regulation, consumer protection, product safety rules and provisions on copyright would therefore all apply as *lex specialis*.[2045] Common transparency reporting obligations, the nomination of contact points or legal representatives for all intermediaries, as well as detailed notice and action (NTD) and counterclaims procedures for hosting providers are new obligations that do not come as a surprise. Notice and action, counterclaims and transparency reporting procedures can be seen as baseline requirements that have been widely demanded. Online platforms are subject to additional, largely procedural, obligations relating to complaints handling, dispute resolution, the use of trusted flaggers, repeat infringements and sanction processes, law enforcement cooperation and transparency reporting on automated content moderation and advertising display. This will doubtlessly help creating additional internal processes, structures and systems which force platforms to build and organise their awareness and knowledge of potential illegal content and activity, and incorporate this into the wider corporate epistemology which informs decision making. The additional requirements for marketplace operators to put KYC-style verification processes of traders in place (Article 22) has

2043 European Commission, 'Commission Staff Working Document - Impact Assessment - Annexes - Accompanying the Document Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC - Part 2' (2020) 161–162 <https://ec.europa.eu/digital-single-market/en/digital-services-act-package> accessed 8 January 2021.

2044 Cole, Etteldorf and Ullrich (2021) (n 548) 186–200.

2045 European Commission DSA proposal (n 10) Article 1 (5), Recitals 9 - 11.

been positively commented on in Chapter 4's sections on trademarks and product and food safety. This ties in with existing due diligence obligations that already exist in the area of consumer law and anti-money laundering compliance. For online marketplaces, this bolsters the general due diligence obligations that are imposed on all online platforms against the misuse of their services (Article 20). However, given that content management processes of other online platforms, such as social media networks or UGC platforms are also capable of posing significant harms, such enhanced verification measures may also be appropriate for these types of platforms, for example when addressing the risks related to user anonymity.[2046]

It is also positive that the DSA takes up the idea of risk management due diligence obligations, data access and compliance scrutiny rights by external, academic researchers, and additional transparency and consumer empowerment options relating to recommender systems, advertising and reporting.[2047] However, requiring these measures only from VLOPs may be a missed opportunity, in particular where it concerns the risk management obligations. For one, it has been shown that the identification of systemic or high risks to public interest and fundamental rights should be a practice embedded into the business planning of every corporate actor. These are basic features of socially responsible and sustainable business management. Secondly, it has been shown that systemic risks may also arise from platforms that are not "very large." Content dissemination happens at a fast and almost uncontrollable speed, making smaller online platforms also prone to causing harms and damages to public interests. This has, for example, been an observation in the area of terrorist content online.[2048] The new audit obligations (Article 28) in conjunction with the risk management obligations and the requirements to appoint compliance officers will likely lead to the emergence of a future GRC system for VLOPs. Large international audit and compliance service providers can be expected to jump on the opportunity to incorporate these kind of systems into their existing service offers. However, the risks of removed technical compliance systems, whereby the private sector audits the private sector, have been outlined above. This should not absolve the regulator from building their own capacities to perform technical and systemic oversight and enforce-

2046 Cole, Etteldorf and Ullrich (2021) (n 548) 182–183.
2047 European Commission DSA proposal (n 10) Articles 25 - 33.
2048 OECD, 'Current Approaches to Terrorist and Violent Extremist Content among the Global Top 50 Online Content-Sharing Services' (n 1090) 6–7.

ment functions. The solutions proposed by the DSA in Articles 28 should therefore be only be a first, transitory step that helps regulators in the acquisition of their own technical auditing skills and capacities.[2049]

Finally, the DSA proposal continues to rely on self-regulatory codes of conduct and best practice sharing as a means of implementing the provisions of the DSA (Articles 34 to 37). However, as has been shown throughout this work, the success of these kind of arrangements has been questionable, at least. If this approach is to be maintained, it would have to be accompanied by more solid regulatory coercive powers, with the option to move towards co-regulatory structures. The use of (technical) standards, as largely advocated for in this work, is limited to more technical areas in the DSA proposal, i.e. to notice-and-action, audits and external information access and exchange requirements. However, little stands in the way of basing complaints handling, sanctions and abuse prevention systems, trader traceability requirements, recommender system due diligence or general systemic risk assessment and control on (harmonised) technical standards. In addition, the multitude of sectoral, national regulators that are likely to be involved in the horizontal supervision of the due diligence obligations spelled out in the proposal, calls for more incisive powers than promotion of best practice sharing and codes of conduct.

2049 Cole, Etteldorf and Ullrich (2021) (n 548) 199.