ACCEPTED VERSION (without final proof edits) of publication in ***International Journal of Law and Information Technology IJLIT, 27 July 2018 (https://doi.org/10.1093/ijlit/eay008***

A risk-based approach towards infringement prevention on the internet: adopting the anti-money laundering framework to online platforms.

Carsten Ullrich[*♣]

Abstract

This paper suggests a new approach towards online service provider liability which relies on duty of care. It proposes a concrete compliance framework for online platforms, borrowed from risk regulation, and modelled on anti-money laundering (AML) obligations in the financial sector. First, the prohibition on obliging platforms to monitor content in a general manner under the E-Commerce Directive will be discussed. On the face of it this may clash with a standardized requirement to filter for infringing content. Subsequently, the regulatory choice for such a duty of care standard will be explored. It is argued that the largely self-regulatory proposals currently on the table may be ill fitted to achieve traction and accountability. Finally, a three-tier compliance framework, modelled on the AML system and using a risk-based approach, is proposed. The pitfalls of such a highly automated compliance solution, which enforces complex legal norms, will also be touched on.

Keywords: intermediary liability, duty of care, risk regulation, co-regulation, anti-money laundering, compliance technologies, algorithmic accountability, regulatory governance

1. Introduction

For over 20 years the internet has been revolutionising the way we do business, create and exchange information. Information service providers (ISPs) who enable access to information on the internet and information uploaded by users and businesses have occupied a centre stage of the so-called platform economy. We know these hosts as social networks, user generated content platforms, search engines or online marketplaces, to name but a few[1]. Since the E-Commerce Directive (ECD)[2] of 2000, these platforms have been enjoying wide-reaching liability exemptions for illegal content hosted on their servers if they act as neutral and passive information hosts and

[*] LLM (Edinburgh), PhD candidate in Law under the supervision of Prof. Mark Cole at the Doctoral Training Unit on Enforcement in Multi-Level Regulatory Systems (DTU REMS), Faculty of Law, Economics and Finance (FDEF), University of Luxembourg

[♣] The author would like to thank Prof. Dr. Mark Cole and Dr. Gavin Robinson (both University of Luxembourg) and Dr. Justin Jütte (University of Nottingham) for their invaluable feedback on the drafts of this article.

[1] Additional platform models are cloud services, collaborative economy platforms, news aggregators or online gaming platforms.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 187 2000. Articles 12 - 15

remove illegal content they are notified or otherwise aware of expeditiously. This protection was initially provided in a bid to protect and promote an emerging and promising innovative economic sector. The sector has indeed been growing successfully and is about to transform almost all sectors of our economy and society at large. Powerful global internet corporations have emerged. But as is common with new, revolutionary opportunities they also disrupt and subvert more traditional sectors and open the door for new and old kinds of abuse. As a consequence, there are now more and more voices, including the EU Commission, who call for internet intermediaries, or online platforms, to be more proactive in helping to prevent unlawful content and activity on the internet[3]. However, it is proving difficult to adjust the current liability protections and to promote a transparent and consistent use of infringement prevention methods across this sector. The now powerful internet corporations have become used to the wide-reaching privileges they enjoy. Moreover, lawmakers find it difficult to regulate in an area that is characterised by complex and fast moving technological advances and where algorithmic decisions taken by these platforms not only filter content, but also dynamically influence information access and display. Meanwhile, curtailing the liability privileges unduly may negatively affect fundamental rights, such as freedom of expression or privacy. Current attempts to regulate have therefore mainly relied on self-regulatory mechanisms, which either encourage infringement prevention technologies, or propose to mandate their use by relying on agreements struck between private actors with little regulatory oversight[4]. As will be shown below there are inherent deficiencies and risks with such an approach.

This paper will draw on the concept of duty of care, to suggest a risk management standard for infringement prevention relying on co-regulation. It will propose a concrete compliance framework for infringement prevention modelled on the existing compliance framework of anti-money laundering (AML) in the financial sector. For this, the following section will discuss the prohibition of requiring intermediaries to monitor content for infringing activity on a general basis, which is part of the current liability framework for ISPs[5]. There is a potential clash with a platform obligation to filter for infringing content as proposed in this paper. The aim of this section is to

[3] EU Commission, 'Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms, COM(2017) 555 Final'.
[4] See Sub-section 3.1.
[5] ECD (n 2). Article 15

critically assess the validity today of Article 15 ECD. The third section will explore how such a due diligence system should be set up in a regulatory context given the powerful and new roles online intermediaries have become to play. The role of soft law and co-regulation, such as technical standards, will be explored in more detail. The fourth section will propose a conceptual design for a standardised duty of care, using a risk based approach to transaction monitoring. The current EU and international anti-money laundering (AML) compliance framework mandated in the financial sector[6] will be analysed with a view to applying it to a due diligence model for infringing content prevention. It is the overall objective of this paper to advance the debate over online intermediary responsibilities beyond pure theoretical reasoning and explore some practical avenues. As will be seen below, state actors and industry have made practical steps in suggesting self-regulatory models. By exploring a co-regulated infringement prevention and removal solution, with public oversight over the technical decision-making process, this paper tries to remedy some of the perceived deficiencies of a largely self-regulatory system. The new nature of the internet has become a breeding ground for innovative and experimental regulatory approaches[7] and this paper hopes to present such an approach.

2. Infringement prevention, duty of care and general monitoring

As a matter of brief introduction, I will quickly outline the current content liability framework applying to online platforms. The below assumes that most of today's online platforms would be defined as information society service providers (ISPs), which means that they offer their services for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[8]. Under the ECD, ISPs enjoy far reaching immunities against infringing content on their

[6] Directive 2015/849/EU of the European parliament anf of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 2015.

[7] Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011) 8–14. And Wolfgang Kerber and Julia Wendel, 'Regulatory Networks, Legal Federalism, and Multi-Level Regulatory Systems' (2016) 13–2016 <http://ssrn.com/abstract=2773548> accessed 6 April 2017. This is just a snapshot of authors who discuss in more detail how the new nature of the internet challenges regulatory enforcement and calls for new, experimental self and co regulatory approaches.

[8] ECD Art 2(a) refers to this definition of an ISP as laid down in Directive 98/34, Art 2 (1). This directive was replaced by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 2015 para 1 (1). The relevant Article is now 1 (1). The majority of today's online platforms would

servers, under certain conditions. These liability exemptions are regulated in Articles 12 - 14, ECD: Article 14 applies to information hosts, or online platforms[9]. According to this, ISPs enjoy these exemptions if they are passive in the sense that they play a mere technical and automated role with regards to the content on their platforms. The idea is that this kind of hands-off involvement does not confer any control or knowledge over the information, including its potential illegality, shared by these information hosts. Consequently, they cannot be held liable for any damages caused by hosting this content. They would just need to act expeditiously to remove illegal content when notified of its existence. In addition, they may be asked to prevent the notified content reappearing on its platform. Article 15 ECD, on the other hand, ensures that ISPs cannot be asked to monitor platform traffic at a general level in order to prevent infringements. Article 15 ECD has been advanced by the CJEU but also national courts when limiting the obligations of ISPs for preventing or policing specific infringements, which are possible under Article 14 ECD[10].

So when arguing about whether intermediaries may be asked to be more proactive in preventing the occurrence of infringing content on their platforms, one inevitably needs to discuss Article 15 ECD. This Article, which precludes member states from imposing on ISPs an obligation to monitor their traffic on a general basis is generally used against widening infringement prevention obligations[11]. As this paper will propose a solution which explores more proactive infringement prevention obligations, it could potentially be seen as in conflict with the current prohibition to require general monitoring. This paper submits that at least acritical re-evaluation, if not abolishment of Article 15 ECD is needed: 1) the underlying economic assumptions for justifying it have changed, 2) the term "general monitoring" is ambiguous in view of the technologies available today[12].

---

meet these criteria. The recent judgement by the CJEU on Uber (*Asociación Profesional Élite Taxi v Uber Systems Spain SL, C-434/15* [2017] ECLI:EU:C:2017:981 (CJEU).provides a useful delineation in this respect.

[9] ibid. Articles 12 and 13 apply to internet access providers, so called "mere conduits", and to caching, respectively.

[10] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, C-360/10* [2012] ECLI:EU:C:2012:85 (CJEU).para 38; *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (Scarlet Extended), C-70/10* [2011] ECLI:EU:C:2011:771 (CJEU). para 40, *L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd and others, C-324/09* [2011] ECLI:EU:C:2011:474 (CJEU)., para 139 ; *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14* [2016] ECLI:EU:C:2016:689 (CJEU). para 87

[11] See further below in this section

[12] Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International BV 2017) 473–474.

In search for a justification of Article 15 the most forthcoming source from the Commission is its first report after the implementation of the ECD, published in 2003. Here, the Commission gives mainly economic reasons for Article 15, such as protecting intermediaries against unreasonably high burdens incurred from checking millions of sites in the face of ineffective filtering technology. [13] The negative impact on freedom expression was seen as an additional risk resulting from ineffective filtering and blocking technology. The predominantly economic justification of Article 15 has been taken up until recent by the Northern Irish Court of Appeals in *CG v Facebook*[14]. Other sources see Article 15 mainly as a means to preclude the creation of actual knowledge and awareness, which would result from imposing more general proactive monitoring obligations, thus limiting the effectiveness of Articles 12 -14[15]. The potential conflict of Article 15 with Recital 48 ECD, which allows Member States to impose on ISPs duties of care as specified in their national law in order detect and prevent infringements, has also been noted[16]. Other documents from the drafting phase of the ECD as well as later reports post-implementation do not shine more light on this matter[17]. In summary, the justifications for Article 15 seem to rest mainly on a desire to protect a nascent ISP sector from overly high burdens of manual verification. It ensures the availability of Articles 12 -14 with their focus on tying liability to actual knowledge of infringing activity gained ex-post, and failure to restrict it expeditiously.

While general monitoring in itself is habitually identified for its potential to have a detrimental effect on fundamental rights, the usability of Article 15 for shielding against this abuse is

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

[14] *CG v Facebook Ireland Ltd & Anor* [2016] 2016 NICA 54 (Court of Appeal in Northern Ireland) [53, 55].

[15] Alfred Büllesbach (ed), *Concise European IT Law* (2nd ed, Kluwer Law International ; Sold and distributed in North, Central and South America by Aspen Publishers 2010) 333. The same source notes that such a general monitoring would be likely to violate privacy rights under the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 Article 8(1). For a more detailed discussion see also Angelopoulos (n 12) 107.

[16] Gerald Spindler, Fabian Schuster and Katharina Anton (eds), *Recht Der Elektronischen Medien: Kommentar* (2 Aufl, CH Beck 2011) 1511. and Arno R Lodder and Andrew D Murray (eds), *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing 2017) 53.

[17] Thibault Verbiest and others, 'Study on the Liability of Internet Intermediaries, Markt 2006/09/E'. p.4-5, This reports repeats the justification of the earlier European Commission report (n 13). EU Commission, 'Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document , SEC(2011) 1641 Final' 47–51.

inconsistently documented. In *SABAM* and *Scarlet*, the CJEU first states that Article 15[18] protects against a general monitoring obligation. It then engages in a balancing exercise[19] between the intellectual property right and other fundamental rights – such as the right to conduct business (in conjunction with the Intellectual Property Enforcement Directive (IPRED)[20]), the right to protection of personal data and the right to impart and receive information. The CJEU rests its balancing exercise on the fact that the right to protection of intellectual property is not inviolable[21] and would need to be balanced against these other fundamental rights. A general monitoring obligation would contradict IPRED, Article 3, which states that the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights must be fair, proportionate and not excessively costly[22]. Article 15 does not appear to play a direct role when conducting a balancing exercise of the fundamental rights for determining the scope of injunctions for infringement prevention. Arguably, therefore, not having Article 15 would change little in engaging in a successful balancing with fundamental rights when determining the scope of injunctions concerning infringement prevention. By contrast, if for any reason a Court's balancing exercise would arrive at an outcome that justifies the imposition of more proactive infringement prevention techniques[23], for example in the light of available technology, Article 15 could still prevent this outcome. The EU Commission already formed a similar view by reasoning that the availability of perfectly effective and costless filtering technology would make Article 15 superfluous[24]. While this is not the case today, it cannot be denied that filtering technology has advanced significantly since the early days of the internet. However, the availability of less intrusive monitoring technology may address some human rights concerns. The inflexibility of Article15 and its ambiguity over the border between general monitoring and specific infringement prevention measures however prohibits such considerations fully.

[18] *SABAM v Netlog* (n 10) [38] *Scarlet Extended* (n 10) [40].
[19] *SABAM v Netlog* (n 10) [39-51] *Scarlet Extended* (n 10) [41- 50]
[20] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 2004 para 3(1).
[21] *SABAM v Netlog* (n 10) [41] *Scarlet Extended* (n 10) [43]
[22] *SABAM v Netlog* (n 10) [34] *Scarlet Extended* (n 10) [36]
[23] keeping in mind that there is no clear definition of general monitoring; see also further below in this Section
[24] EU Commission, 'Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document , SEC(2011) 1641 Final' (n 17) 50.

On a more technical level, and as can be seen from later reports by the EU Commission in 2007 and in 2012[25], various Member States and national courts have continuously had difficulties in deciding when a specific infringement prevention turns general. If a platform is held to prevent any kind of similar infringement (and case law has been differing on the broadness of the term "similar"), would all uploaded content not need to be filtered to ascertain that it did not constitute that similar infringement? And is that content verification process actually an act of monitoring? Maybe the technical dimension of filtering has evolved in a way that makes monitoring or content checking less costly and intrusive[26]? This lack of clarity continues and has been repeatedly documented[27]. The controversial proposal of the EU for a new Copyright Directive[28] and the Audiovisual Media Services Directives (AVMSD)[29] also show that the EU has not been able to

[25] Verbiest and others (n 17). EU Commission, 'Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document , SEC(2011) 1641 Final' (n 17).

[26] For example, in the area of filtering for copyright infringing content, apart from You Tube's proprietary filtering solution, Content ID ('How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en> accessed 28 September 20170. There are other solutions available on the market used by ISPs: Audible Magic, 'Copyright Compliance Service Compliance Automation for Media Sharing Platforms' <https://www.audiblemagic.com/compliance-service/#pricing> accessed 5 March 2018. And Institut National de l'Audiovisuel, 'Ina-Signature : Protégez et Gérez Vos Contenus' <https://www.ina-expert.com/content/download/2103/44165/version/latest/file/1> accessed 5 March 2018. Moreover there are now a considerable number of companies which offer internet filtering solutions for detecting IP infringing content for rights owners. These can also be employed by platforms or ISPs to detect infringements. Some of the more known solutions are from companies such as Gracenote. MarkMonitor, Vobile, Nagra Kudelski. Meanwhile research in text and image recognition as well as artificial intelligence in fraud detection are booming and throw up the question of the possible public sector involvement in supporting the development of a market for such technology: see for example Lital Helman and Gideon Parchomovsky, 'The Best Available Technology Standard' [2011] Columbia Law Review 1194.

[27] See for example the discussion regarding German case law in: Georg Nolte and Jörg Wimmers, 'Wer Stört? Gedanken Zur Haftung von Intermediären Im Internet – von Praktischer Konkordanz, Richtigen Anreizen Und Offenen Fragen' (2014) 16 GRUR 21–23. For a wider discussion on the matter: D Friedmann, 'Sinking the Safe Harbour with the Legal Certainty of Strict Liability in Sight' (2014) 9 Journal of Intellectual Property Law & Practice 148, 152–155. and Peggy Valcke, Aleksandra Kuczerawy and Pieter-Jan Ombelet, 'Did the Romans Get It Right? What Delfi, Google, EBay, and UPC TeleKabel Wien Have in Common', *The responsibilities of online service providers* (Springer Berlin Heidelberg 2017) 11. and Angelopoulos (n 12) 100–107. but also the recent referral of the Austrian Supreme Court to the CJEU where the former asks for guidance on whether Art. 15(1) ECD conflicts with an injunction against Facebook to prevent defamatory language similar to previously notified comments, *Glawischnig-Piesczek, v Facebook, 6Ob116/17b* (Oberster Gerichtshof, Republik Österreich) and *Glawischnig-Piesczek, C-18/18* (CJEU) Pending Case.

[28] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market, COM(2016) 593 final 2016. Article 13

[29] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final 2016. Article 28a

obtain that clarity so far. Moreover, these questions may be even more difficult to answer for new business models in the collaborative or platform economy[30], which is characterised by more complex interactions in multi-sided markets[31]. Big data, generated on platforms can now more readily be analysed and interpreted. It is the question whether, for example, content recognition technologies, which process and analyse large amounts of content in an automated and more transient way constitute general monitoring. It has been argued that, for example, less intrusive, "shallow packet inspection" could escape the classification as general monitoring. It would all depend on the definition of "general monitoring"[32]. Meanwhile, algorithmic decision making today, as for example used in the recognition and distribution of content on the internet, although processing personal data "at some level" do not necessarily and always impinge on privacy[33]. The new General Data Protection Regulation could prevent that content filtering systems retain any data beyond the necessary, i.e. to execute takedowns and effectively enforce[34].

However, he above demonstrates the dilemma of trying to define more concrete duties of care for detecting and preventing illegal activities, which can be reasonably expected from diligent economic operators. Nevertheless, such duties of care may not only be necessary in the face of diverging national interpretations[35], but also because of the diversification of the intermediary sector and its ever-growing importance. Waiting for national courts to develop such guidelines out of the national transpositions of the ECD, or waiting for the CJEU to harmonise differing interpretations may not be a wise choice given the rapid speed of development in the sector. The principle of duty of care meanwhile is well anchored in both civil and common law traditions and used across a wide variety of legal fields. In addition, the European legislator has provided an argument for Member States to explore duties of care under ECD Recital 48. With this is in mind,

---

[30] Yolanda Martinez Mata, 'Bolkestein Revisited in the Era of the Sharing Economy' [2017] Revista Electrónica de Estudios Internacionales 7 <http://www.reei.org/index.php/revista/num33/notas/bolkestein-revisited-in-the-era-of-the-sharing-economy> accessed 12 September 2017.

[31] Olivier Sylvain, 'Intermediary Design Duties' 58 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997141> accessed 19 September 2017.

[32] Angelopoulos (n 12) 473–474.

[33] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to Explanation"Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18, 82.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC 2017 Article 25: the Data protection by design and by default provision

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

the proposal offered in this paper assumes that a clear-cut decision on whether it conflicts with a present-day interpretation of Article 15 is not possible. Moreover, it intends to highlight the obsolescence of the current liability framework[36]. The technological progress with regards to content filtering and the economic status of the industry might justify a review of this 20-year old provision.

3. Duty of care and the regulatory choice

3.1. Current duty of care proposals – a review

The idea of using the duty of care principle for obliging online platforms to participate in more proactive infringement prevention is not new. Several authors have by now explored it. *Leistner*[37] suggests compiling common principles of intermediary secondary liability derived from a repository of EU Member State case law where preventive measures where imposed on ISPs. These would be developed into a reasonable duty of care standard. However, he is critical of this being a self-regulatory solution. *Helman and Parchomovsky*[38] and *Verbiest/Spindler*[39] develop the idea of technology based safe harbours, where duty of care is tied to the use of state-of-the-art filtering technology. Both suggest co-regulatory solutions, namely through standardization, to create statutory oversight over the development and use of the technology. This is meant to ensure a level playing field between intermediaries and transparency over the decision-making mechanism (algorithm). An obvious challenge to this solution is that, the wider the insights and participation in this filtering algorithm, the higher the likelihood that that the detection technique will be disclosed, opening the door for circumvention and abuse. Therefore an open source model for filtering technology, for example, may be counterproductive in this area[40]. *Valcke et al* look at the example of (self-regulatory) ethical codes drawn up by press associations or journalism

[36] See also: Sophie Stalla-Bourdillon, 'Internet Intermediaries As Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well.', *The responsibilities of online service providers* (Springer Berlin Heidelberg 2016) <http://link.springer.com/10.1007/s11948-015-9734-1> accessed 17 February 2017. Giancario F Frosio, 'The Death of No Monitoring Obligations' (2017) 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 199.

[37] Leistner (n 31) 88–90.

[38] Lital Helman and Gideon Parchomovsky, 'The Best Available Technology Standard' [2011] Columbia Law Review 1194, 1225.

[39] Verbiest and others (n 17) 19–23.

[40] Martin Husovec, 'Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13' <http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/> accessed 28 September 2017.

councils as a possible model for a duty of care standard for ISPs. Courts would take these standards as a yardstick when deciding on content liability cases involving ISPs. In the US, *Citron et al*[41] meanwhile argue for a narrower interpretation of the liability exemptions provided under the Communications Decency Act[42]. That defence should only be available to Good Samaritans, i.e. those ISPs who already display a level of duty of care with regards to preventing and removing infringing content[43]. That duty of care standard would be dependent on the nature and size of the platform activities and it would evolve in line with improvements in filtering and blocking technology[44]. However, the authors leave open who would set that standard and who would assessed it for its adequacy. *Lavi* looks at social media and UGC platforms and proposes a context based differentiation of liability immunities[45]. *Waismann et al* define a flexible standard of duty care for search engines based on reasonableness. That reasonableness depends on cost, scope, potential harm and impact on fundamental rights[46].

The above examples show that there is an emerging opinion on how to involve ISPs more proactively in preventing and combatting third-party infringing content. At the same time there seems to be less consensus over the type of regulatory intervention needed. Beyond the above ideas there have been no concrete proposals on the compliance framework and risk management framework which could be used to implement such new duty of care standards.

Looking at the regulatory choice, it appears that at least the EU Commission has set its mind on a mix of self- and co-regulation, relying heavily on industry-driven codes of conduct and information sharing. In its recent proposals for a Copyright Directive[47] the EU Commission

[41] Danielle Keats Citron and Benjamin Wittes, 'The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity' (2017) University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2017-22 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007720> accessed 18 September 2017.
[42] The Communications Decency Act (CDA) 1996, section 230
[43] Currently the CDA (section 23Communications Decency Act of 1996 (CDA)0) protects those ISPs which act as Good Samaritans against any liability for illegal content which they attained knowledge of due to their prevention activities. Other ISPs, however, still enjoy unduly broad immunity even if they do not display any duty of care, according to Citron et al. Citron argues for a reinterpretation of section 230, affording only those ISPs which act as Good Samaritans immunity. Note that this Good Samaritan defence does not exist in the EU.
[44] Citron and Wittes (n 37) 17.
[45] Michal Lavi, 'Content Providers' Secondary Liability: A Social Network Perspective' (2015) 26 Fordham Intell. Prop. Media & Ent. LJ 855.
[46] Augustin Waisman and Martin Hevia, 'Waismann Theoretical Foundations of Search Engine Liability' (2011) 42 International Review of Intellectual Property and Competition Law 785.
[47] Copyright Directive Proposal (n 25). Article 13, Recital 38

mandates the use of filtering technologies. It prescribes cooperation and information sharing between platforms and rights holders, and encourages best practice sharing between both parties. In the area of hate speech and terrorist content regulatory efforts rest on a (non-binding) code of conduct between major social media platform operators[48]. The same is true for the fight against counterfeit products on the internet where the Commission merely facilitates stakeholder action based on a broad Memorandum of Understanding between major brand owners and e-commerce platforms[49]. In the amended AVMSD[50] the Commission is arguably closest to a co-regulatory mechanism. While it obliges video sharing platforms to take appropriate measures to protect users against illegal content, it also charges the European Regulators Group for Audiovisual Media Services (ERGA) with facilitating and advising during the creation of EU wide codes of conduct and best practice sharing.

According to these proposals the actual influence over extent and nature of the infringement prevention and detection remains largely in the hands of platforms and industry stakeholders (such as rightsholders). Whether this type of intervention can still be termed self-regulation or is already co-regulation is open to wide discussion[51]. There is an impressive array of typologies which look to classify various approaches to regulatory topics on the internet (e.g. content regulation, advertising, data protection, communication protocols, consumer protection) by their degree of involvement by state and industry actors[52]. None of the current regulatory approaches and solutions in the EU include a formal element of mandatory statutory review, approval or audit of the solutions that are (to be) proposed by industry. They are therefore more likely to qualify as self-regulatory rather than co-regulatory solutions[53]. The recent Communication of the EU

[48] 'European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech' <http://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 9 March 2017.

[49] 'Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet, 2011'. This Memorandum was renewed in 2016 as stakeholders agreed on common key performance indicators with regard to the fight against infringements.

[50] Proposed AVMSD amendment (n 26). Recital 37, Articles 4(7); 28a(7) & (8); 30a

[51] LAJ Senden and others, *Mapping Self-and Co-Regulation Approaches in the EU Context'': Explorative Study for the European Commission, DG Connect* (European Commission 2015) 20–31 <http://dspace.library.uu.nl/handle/1874/327305> accessed 10 March 2017. Gerald Spindler and Christian Thorun, 'Die Rolle Der Ko-Regulierung in Der Informationsgesellschaft' (2016) 6 MMR-Beil. 1, 5.

[52] Marsden (n 7) ch 2. Contains a comprehensive discussion of these regulation typologies for the internet.

[53] In Marsden's (ibid 63, 227.) Beaufort scale of self- and co-regulation the current approaches would vary between level 2 – 5 and thus squarely fit within self-regulation (Level 11 would constitute "classic" co-regulation. According to Spindler and Thorun (n 47) 8–9, these approaches would fit within their definition of self-regulation. The

Commission on tackling illegal online content on platforms[54] is a tentative step in the direction of a co-regulatory mechanism as it encourages co-operation of platforms with law enforcement and for the first time and encourages explicitly the use of state-of the art filtering technology and technical surveillance technology. The encouragement of platforms to create and publish transparency reports on notice and takedown actions[55], and the desire to standardize these, could however be a useful foundation for mandatory, and co-regulated obligations. It remains to be seen whether this approach will be followed by the Commission's upcoming communication, announced for spring 2018, on fake news and online disinformation[56]. The EU is currently analysing the self-regulatory measures it encouraged platforms to take in 2016 to fight hate speech[57] and may propose legislative intervention.

3.2. Self- or co-regulation?

There are several reasons for the current prevalence of self-regulatory models on the internet. The most common, distilled from the variety of literature available on this topic appear to be: 1) the capability challenge faced by regulatory and enforcement authorities: the sheer amount of content, the unprecedented level of technical skills needed to understand internet businesses, plus the speed with which the industry develops[58] lead to the state assigning more regulation tasks to the private sector; 2) the new cross-cutting nature of the internet and the emerging multi-sided platform economy requires new interdisciplinary and innovative, regulatory tools which can be a problem with regulators whose scope of activity is firmly prescribed[59], 3) a cultural tradition in certain

proposed approach in the AVMSD however is likely to be on the edge towards co-regulation, due to the quasi-mandatory involvement of ERGA.

[54] EU Commission, 'Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms, COM(2017) 555 Final' (n 3).

[55] ibid 16.

[56] EU Commission, 'Next Steps against Fake News: Commission Sets up High-Level Expert Group and Launches Public Consultations, IP/17/4481' <http://europa.eu/rapid/press-release_IP-17-4481_en.htm> accessed 22 December 2017.

[57] EU Commission, 'Commission Updates EU Audiovisual Rules and Presents Targeted Approach to Online Platforms, IP/16/1873' <http://europa.eu/rapid/press-release_IP-16-1873_en.htm> accessed 22 December 2017.

[58] Jason Freeman, 'Consumer Legislation and E-Commerce Challenges' (2015) 2 Rivista Italiana di Antitrust/Italian Antitrust Review 80 <http://iar.agcm.it/article/view/11380> accessed 19 September 2017. Julie E Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369. Cohen shows how "infoglut" and fast paced technological change have outpaced regulatory capacities. Spindler and Thorun (n 47) 6.

[59] Cohen (n 54) 375–387. Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487, 496.

European countries[60] or varieties of capitalism[61] which is conducive to collaborative regulatory structures between the state and industry, especially in new and emerging industry sectors.

At the same time, the risks of self-regulatory models for the internet are increasingly discussed[62]. With regards to content regulation a major criticism refers to a loss of democratic control and accountability over enforcement if the private sector is left to its own devices to regulate. As powerful internet actors define and enforce their content policies largely based on commercial interest criteria and continue to enjoy far reaching immunities their activities risk being above the law[63]. Nevertheless, these companies need to and will react to local regulators and cultural sensibilities regarding for example offensive material. However, with the current protection they may be able to choose and pick, and alternatively claim ignorance over the existence of the content, or overzealously remove it following a risk and cost benefit analysis[64]. This trend is exacerbated by new, dynamic gatekeeping roles of platforms the effects of which are not yet fully understood[65]. These gatekeeping mechanisms may affect different users in a different way and diffuse an understanding of their real impact. They are however ultimately driven by commercial interests to optimise network effects, attract traffic and lock-in old and new users[66]. They therefore compound concerns over market dominance related to new gatekeeping powers[67], while protecting opaque and inadequate content management activities.

These trends have led to renewed calls for stronger state oversight through co-regulatory arrangements[68]. The debate over a review of the intermediary liability regime is directly related to this. As discussed in the previous section, the thrust of the debate should be to forego or relax the

[60] Senden and others (n 47). This study identifies the UK, Germany, the Netherlands and to some extent Italy with strong traditions in co- and self-regulatory practices.
[61] Marsden (n 7) 67–70. Marsden cites Rhinish and Scandinavian capitalism as conducive to co- and self-regulation, and outlines marked differences to US regulatory styles.
[62] Co-regulation, depending on definition and the degree of involvement of state actors, is more ambivalently discussed than self-regulation. In fact co-regulation is both seen as suitable remedy to self-regulation (Spindler and Thorun (n 47). Marsden (n 7) ch 8.; Florian Saurwein, Natascha Just and Michael Latzer, 'Governance of Algorithms: Options and Limitations' (2015) 17 info 35, 42.)
[63] Pasquale (n 55) 496.
[64] ibid 497.
[65] Natali Helberger, Katharina Kleinen-von Königslöw and Rob van der Noll, 'Regulating the New Information Intermediaries as Gatekeepers of Information Diversity' (2015) 17 info 50. According to this typical gatekeeping features are for example content personalization, enhanced connectivity features or differentiated user rights.
[66] Sylvain (n 28) 59.
[67] Cohen (n 54) 376–378.
[68] Saurwein, Just and Latzer (n 58) 40–42.

distinction between specific and general monitoring, and "passive" and "active" hosts and concentrate on reasonable duties of care. It is clear immediately that the debate on duty of care really is about prescribing or bringing to light activities that online platforms need to perform as diligent economic operators. The call for duties of care, whatever their design, goes hand in hand in with demands for publicly controlled governance and transparency common to other economic areas faced with similar transformation caused by new technological disruption and information management. Examples are the financial industry, environmental management, or technical and safety requirements concerning products.[69].

Where the state tries to gain more regulatory control it needs to counter the pressures which have previously forced the prevalence of self-regulatory models mentioned above. The complexities involved in overseeing these areas have led to a demand for new governance models. Regulators must be able to understand and keep pace with the new institutional self-regulatory models that have arisen out of these industries. These models are characterised by standard and norm setting through informal procedures, managed by professional and technical expertise networks[70]. Therefore, to merely "be part of the process" and facilitate self-regulatory efforts characterised for example by best practice and code of conduct facilitation is not enough. Regulatory activity needs to move further, into the sphere of auditing, standard setting, compliance reporting[71] and decisional accountability[72]. The latter concepts acknowledge that in these information and technology driven industries, which require complex decision making, legal compliance also entails complex decisions. Traditional rules-based compliance is too static and ill fitted to achieve desired policy outcomes.

Decisional accountability means then that regulatory risk management is being embedded in the technology and the algorithm itself[73]. This means that the regulated entity to needs to demonstrate that its technology choices were sufficiently informed by regulatory requirements and public interest obligations. The emphasis is on good, responsible and transparent decision-making. It

[69] Cohen (n 54) 395.
[70] ibid.
[71] ibid 403.
[72] Kenneth A Bamberger, 'Technologies of Compliance: Risk and Regulation in a Digital Age' (2009) 88 Tex. L. Rev. 669, 684.
[73] ibid 684–685.

enables the regulator to have constant oversight and intervene as necessary[74]. For example, in the financial sector, obligations in the area of anti-money laundering mean that regulated entities need to document their (obligatory) risk assessments[75] and apply a risk-based transaction monitoring process for suspicious activity. The (documented) internal procedures for suspicious transaction monitoring would form the basis for the algorithms used in a transaction monitoring systems. Finally, system performance would be tested for compliance with those internal procedures, ensuring the programmers implemented internal guidelines adequately into the algorithm[76]. This means however, that regulators also need to become more technical and at least be able to audit and assess algorithms and complex control software. Meanwhile there is a need to continue to involve sound human judgement at critical points of the algorithmic decision making to counter the institutionalization of risk measurement[77]. This approach is not always and necessarily geared towards achieving 100% legal compliance.

This kind of regulatory governance system could be used for reasonable duty of care standards around content regulation. In fact, and as detailed above, platforms are making these kinds of decisions already and enforce the law, albeit largely unfettered from regulatory oversight. We are therefore looking for a technical compliance framework, which would translate duty of care into risk-based, minimum prevention and takedown requirements.

4. Risk management AML style

4.1. Why use the AML framework?

This Section analyses the regulatory framework of anti-money laundering and counter terrorist financing (AML) in the financial industry with a view for its suitability as a model for a duty of care standard in platform content regulation. Before undertaking a short explanation of the AML

[74] This has led to a boom in the use of automated compliance systems, which are often embedded in companies overall risk management structures, for example as Governance, Risk and Compliance (GRC) systems. Prominent examples are: the financial services sector, where automated compliance systems respond to Basle II, Sarbanes-Ox, or anti-money laundering requirements); manufacturing, with complex environmental and health and safety reporting requirements; export and trade compliance reporting obligations.

[75] Directive 2015/849/EU of the European parliament anf of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 2015 Art. 8 (1, 2).

[76] Dennis Cox, *Handbook of Anti-Money Laundering* (Wiley 2014) 233.

[77] Bamberger (n 68) 712, 736–737. This may lead to inflexibility in the risk monitoring process and neglect of (qualitative) shifts in risk exposure

legislation and its implementation, the reasons for the choice of this regulatory framework will be outlined briefly. After this, the elements of the AML structure which could be adopted to duty of care obligations will be explained.

It is important to state that this comparison is not meant to liken the crime of money-laundering or terrorist financing to unlicensed video uploads, hate speech, the online sale of fake mobile phone chargers or the like. It simply analyses the technical and conceptual suitability of the AML management framework in view of its similarities in the transaction environment and the use of technology with the area of platform content management.

There are several reasons why the AML framework lends itself to the purposes of this exercise:

1) AML applies to a high-volume transactions environment taking place to an overwhelming extent by electronic means[78]. In 2015, 433.1 billion non-cash transactions were recorded worldwide, of which over two thirds happened in the industrialised world[79]. Widely available statistics testify to the high volume character of information content up- and downloads on the internet. For example, You Tube deals with 300,000 uploads every day, which results in 4 million hours of video content. Meanwhile, on Facebook 136,000 photos and over half a minute comments are posted every minute[80].

2) Financial products are highly complex and innovation both in financial service products and means of value transfer are strong. In addition, the circumvention techniques by fraudsters are constantly evolving. Online platforms face similar challenges, caused by complexities in content legislation (e.g. the correct and timely identification of copyright, trademark infringements or hate speech, product legislation in e-commerce) and constantly evolving business models and technologies. To address this complexity transaction monitoring in both areas have moved to

[78] Shijia Gao and others, 'Knowledge-based Anti-money Laundering: A Software Agent Bank Application' (2009) 13 Journal of Knowledge Management 63, 64. Although the first stage of money laundering consist of injecting illegitimate funds, mostly through cash transfers, into the financial system, the subsequent phases of layering (obscuring origin of the funds through complex transaction) and integration (the final conversion of the funds into the official economy) happen within the financial system and would be electronically tracked in one way or another.

[79] CapGemini and BNP Paribas, 'World Payments Report 2017. A Preview into the Global Payments Landscape.' (2017) 6–8.

[80] Domo.com, 'Data Never Sleeps 4.0 - 2016 Data' <https://web-assets.domo.com/blog/wp-content/uploads/2016/06/16_domo_data-never-sleeps-4-2.png> accessed 30 April 2018. Jeff Schultz, 'The Amount of Data Created Each Day on the Internet in 2017' (*Micro Focus Blog*, 10 October 2017) <https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/#> accessed 30 April 2017.

highly complex systems involving real-time monitoring and predictive analysis using artificial intelligence[81].

3) AML happens in an international framework applied throughout the industrialised world, reflecting the globalised nature of the financial industry and capital flows[82]. The global and cross/jurisdictional nature of the internet and online platforms does not need further referencing.

4) Some of the large platforms either own or integrate electronic payment services and would already be involved in or even conduct AML compliance activities.[83] E-commerce marketplaces Amazon and Ebay are regulated as payment and e-money institutions by the Luxembourg financial regulator CSSF. Both Google and Facebook operate subsidiaries regulated as e-money institutions in the UK and Ireland, respectively. These platforms may therefore already be under AML obligations and therefore possess valuable experience, which they could adapt to technical duty of care standards[84]. Apart from that, platforms do already engage in fraud detection and prevention risk as part of their activities[85].

---

[81] Shijia Gao and others, 'Knowledge-based Anti-money Laundering: A Software Agent Bank Application' (2009) 13 Journal of Knowledge Management 63. Noriaki Yasaka, 'Data Mining in Anti-Money Laundering Field' (2017) 20 Journal of Money Laundering Control 301.

[82] 'FATF - Members and Observers' <http://www.fatf-gafi.org/about/membersandobservers/> accessed 22 September 2017. The Financial Action Task Force (FATF) which sets standards and promotes implementation of anti-money laundering activities had 37 members by 2017, of which all industrialized Western nations (EU, Switzerland, North America, Japan) and emerging economies (BRICS – Brazil, Russia, India, China, South Africa) and several others.

[83] Amazon Payments Europe is registered as an electronic money institution with the Luxembourg financial market regulator (CSSF), while Ebay is regulated as a payment institution with the CSSF. https://supervisedentities.apps.cssf.lu/index.html?language=en&type=PIN#SimpleSearch > accessed 30 April 2018 Google Payment Ltd has an E-Money issuer license with the UK Financial Conduct Authority and Facebook Payments International Limited is regulated as an E-Money institution by the Central Bank of Ireland. UK Financial Conduct Authority: https://register.fca.org.uk/shpo_searchresultspage?search=Google&TOKEN=3wq1nht7eg7tr > accessed 30 April 2018, Central Bank of Ireland: http://registers.centralbank.ie/FirmRegisterDataPage.aspx?firmReferenceNumber=C148215&register=38 > accessed 30 April 2018 See also: J Bruce Richardson, 'With Great Power Comes Little Responsibility: The Role of Online Payment Service Providers with Regards to Websites Selling Counterfeit Goods' (2014) 12 Canadian Journal of Law and Technology <https://ojs.library.dal.ca/CJLT/article/view/6607> accessed 20 March 2017.

[84] The cross-cutting nature of fighting illegal activity online and anti-money laundering activities is increasingly commented on. E.g. Cortney Weinbaum, 'Covert Influence Is the New Money Laundering' (2017) <https://techcrunch.com/2017/11/05/covert-influence-is-the-new-money-laundering/> accessed 30 April 2018. Elizabeth Thompson, 'Money Laundering Watchdog Scrutinizes Facebook, Social Media' (2017) <http://www.cbc.ca/news/politics/facebook-twitter-privacy-moneylaundering-1.4020638> accessed 30 April 2018.

[85] See for example: Markus Ruch and Stefan Sackmann, 'Customer-Specific Transaction Risk Management in E-Commerce', *Value creation in e-business management* (Springer 2009).

4.2. The AML framework – a brief overview

By the late 1980s industrialised states had realised that money laundering had become a problem on a global scale which could not be tackled through domestic legislation alone. This was mainly due the accelerating globalisation of capital flows, trade and the digital revolution, which facilitated global information exchange. The G7 states set up the Financial Action Task Force (FATF) in 1989 to coordinate worldwide anti-money laundering efforts. It was charged with developing standards and recommendations and with coordinating the implementation of effective rules to fight threats to the global financial system arising from illegal activities. Subsequently the links of other illegal activities to money laundering, such as tax evasion, corruption or human trafficking, were also realised. With the terror attacks of 09/11 in New York, terrorist financing became an additional focus area of the FATF[86]. The FATF has so far issued five rounds of updated and adjusted guidance and recommendations between 1990 and 2012. These are subsequently being introduced into national laws by its members and beyond[87]. In the EU this has resulted in a series of four anti-money laundering directives since 1990, with the latest having been enacted in 2015[88]. Not only are traditional credit and financial institutions (banks, investment funds, insurance companies) covered by specific obligations, but it also applies to non-financial actors such as casinos or real estate agents, or entities handing large cash transaction[89]. A currently proposed Fifth Directive would see the scope of regulated entities extended to virtual currency platforms and anonymous payment instruments, i.e. custodian wallet providers[90].

In its beginning, the AML framework was more static, obliging regulated entities to report transactions or other suspicious activity according to fixed parameters or thresholds specified by

[86] See for a more comprehensive historical account of the international AML system: Stavros Gadinis and Colby Mangels, 'Collaborative Gatekeepers' (2016) 73 Wash. & Lee L. Rev. 797, 850–874. and Maria Bergström, Karin Svedberg Helgesson and Ulrika Mörth, 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management: A NEW ROLE FOR FOR-PROFIT ACTORS?' (2011) 49 JCMS: Journal of Common Market Studies 1043, 1047–1050;

[87] 'FATF Countries' <http://www.fatf-gafi.org/countries/> accessed 25 September 2017. As per its official webpage 190 jurisdictions have now committed to the FATF recommendations.

[88] Directive (EU) 2015/849 of the European parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 2015.

[89] ibid. Articles 2, 3

[90] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM(2016) 450 final 2016 para 1 (1).

the law[91]. This rules-based system was soon perceived as too inflexible and ineffective as it did not consider the dynamism of risk[92] in this fast-moving and complex sector. It also did not incentivize private actors to engage in their own threat analysis[93]. Following the evolvement of FATF recommendations, the EU introduced a risk-based approach towards anti-money laundering under the Third AML Directive in 2005[94], which was further extended by the recent Fourth Directive[95]. Under this approach financial institutions and other regulated entities are held to engage in ongoing transaction monitoring and risk assessment. In the EU, financial and credit institutions are obliged to apply customer due diligence (CDD) measures to new customers by verifying their identity through document checks and establishing beneficiary ownership[96]. This is commonly referred to as a Know-Your-Customer (KYC) process. Secondly, under CDD they need to conduct ongoing transaction and client status monitoring using a risk-based approach[97]. Thirdly, where they detect activity suspicious of money laundering or terrorist financing they are held to report these to the national Financial Information Unit[98].

While the Fourth AML Directive essentially provides procedural requirements, it leaves the actual risk assessment activity largely to the regulated entities. More technical guidance on how, for

[91] Rules typical impose reporting obligations for specified transaction over a certain threshold

[92] see also Bamberger (n 68) 707–708. on the topic on rules-based compliance systems, the ineffectiveness of purely rules based systems has also been pointed out by Lishan Ai and Jun Tang, 'Risk-based Approach for Designing Enterprise-wide AML Information System Solution' (2011) 18 Journal of Financial Crime 268.

[93] Katalin Ligeti and Maxime Lassalle, 'La Quatrième Directive Anti-Blanchiment: Quels Changements Pour Le Luxembourg?' (2016) 2 Revue luxembourgeoise de bancassurfinance 58.

[94] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing 2005.

[95] Directive (EU) 2015/849 (n 79).

[96] ibid. Article 13 (1) a) -c)

[97] ibid Article 13. (1) d) This means concretely that they need to monitor any change in the risk profile of the customer, products, or geographic exposure and monitor transactions with a view to detecting any activity that could be suspected of money laundering and terrorist finance. See also 'FATF Recommendations 2012 - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 22 September 2017. Recommendation 10 Customer Due Diligence

[98] Directive (EU) 2015/849 (n 79). Articles 32-34. While the 5th AMLD proposal (n 81) returns to more rules-based compliance measures with regards transaction with high-risk countries, it is open to debate whether the risk-based approach will be significantly weakened. After looking at the proposal it is submitted here that in its core that approach is maintained. See in addition: 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)', *Comparative Perspectives on Privacy in an Internet Era*, vol VII (CAP Forthcoming) 25–27.

example, risk assessment could be effectively structured is then issued through recommendation and technical compliance standards by the FATF[99]. Companies were given the obligations as well as the flexibility to perform their own risk assessment according to their product mix, customer base and geographic exposure. It was deemed more effective to allocate the risk management to the companies as they were dealing directly with the customer and had immediate access over all relevant transaction data. This has also led to the regulated institutions developing highly sophisticated risk transaction monitoring software systems[100]. Under the risk-based approach they are now moving increasingly away from entirely rules-based (red flag) transaction monitoring algorithms and supplement these with flexible, risk-based approaches and intelligent, self-learning algorithms to detect fraud patterns[101].

Meanwhile the prevalence of algorithmic decision making in the AML area has also been criticised over lack of (democratic) accountability and procedural transparency as it is enshrined within a hardly penetrable complex technical system[102]. Nevertheless, while a majority of suspicious transaction reports is software generated, they still require human follow up, investigation and explanation with the regulator. It has been argued that this would be a way to balance against defensive and overzealous reporting, as well as address concerns over opacity of the process[103]. Sustained regulator involvement and independent human enquiry into machine decisions could eventually help avoiding self-referential and unaccountable systems, and ensure transparency of the algorithm[104].

4.3. Structuring duty of care obligations

As previously mentioned there are three core elements that can be distinguished in an AML framework: KYC, transaction monitoring (both part of CDD), and suspicious transaction reporting. This paper suggests that, on a modified basis, these could be core components of a horizontally applied duty of care standard for online platforms. The scope of each of these components could then be adapted on a sectorial level, i.e. to the type of content or type of platform

[99] 'FATF Recommendations 2012 - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (n 88).
[100] Gadinis and Mangels (n 77) 809, 882–883.
[101] Gao and others (n 72) 67–69.
[102] Bergström, Svedberg Helgesson and Mörth (n 77). Bamberger (n 68) 727–730.
[103] Gadinis and Mangels (n 77) 886–888.
[104] Bamberger (n 68).

business model. A risk-based approach, making platforms responsible and accountable for their risk assessment while setting the broad parameters of such an exercise, should be another key element of an effective duty of care system which platforms can apply from AML. The below sections will discuss suggested elements of such an approach in the area of infringement prevention in more concrete detail. Where platforms demonstrate compliance with the defined duty of care standard they would be exempt from any content liability. In effect, the duty of care standard would replace the current liability regime of the ECD and eschew the current division between "active" and "passive" hosts as well as the dichotomy of specific and general monitoring.

Standards in this context mean technical standards, which in a co-regulatory approach, would serve as a legally mandated proof of compliance, similar to the "New Approach" used by the EU legislator in the area of product conformity[105]. Product standards rely on a similar conceptual approach, which is based on self-certification but may also, depending on the complexity and risk inherent in the product, prescribe compliance with specific technical and safety requirements defined through European norms. As alluded to above, this flexibility could be applied on a sectoral level when adapting duty of care standards to specific technical platform models and/or types of content. An illustration of such a flexible, three-tier risk management system is given in Figure 1.

It should be noted that the risk-based approach is also applied in other regulatory contexts within the EU. The new General Data Protection Regulation (GDPR) is based on such an approach[106]. It mandates risk assessments of the data processing activities of controllers and processor, and prescribes data protection impact assessment and reporting requirements for high risk activities involving personal data[107]. This fits into the wider picture of modern risk regulation[108] being applied in areas driven by complex technologies and innovation[109].

[105] My approach is based on Spindler and Thorun (n 47) 24. and Verbiest and others (n 17). 20-22

[106] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC 2017.

[107] ibid. For general risk assessment Articles 24(1), 25(1); for data protection impact assessment Article 35

[108] Bamberger (n 68) 673.

[109] See also the discussion in Section 3.2.

4.3.1. KYC and Risk assessment

Within the AML framework the KYC process is performed to identify the customer and enable the application of the risk based approach[110]. Identification checks, beneficiary owner and business purpose verification would allow the entity to decide whether enhanced, standard or simplified due diligence measure would need to be applied to the customer.

The idea of KYC-style customer identification processes for intermediaries or online platforms is not new. In the response to the EU Commission's public consultation on the enforcement environment of intellectual property rights (IPRs), rights owners demanded that such processes be prescribed for intermediaries[111]. Rights owners would like to see such processes on online platforms so that repeat defenders can be adequately sanctioned. For rights owners themselves this would facilitate prosecuting sellers or uploaders for rights infringements. The CJEU has provided a basis for such obligations, for example, in L'Oréal, where it first offered the possibility of a court ordering an online marketplace to suspend the perpetrator of the infringement of intellectual property rights in order to prevent further infringements of that kind by the same seller in respect of the same trademarks if it does not decide to so on its own initiative. [112]. In order to offer effective remedies against intellectual property rights infringers an online marketplace may be ordered to take measures to make it easier to identify its customer-sellers[113]. Protection against repeat offenders requires the possession of the identity of the offending party. In McFadden the CJEU concluded that password protection of a public W-LAN network, which required the internet user to disclose their identity, would be an adequate measure of dissuasion from connections which infringed copyright or related rights[114]. In the e-commerce sector platforms may already be required to apply KYC if they are offering their own payments solutions for sellers and clients.

The KYC requirement for online platforms would serve two objectives:

---

[110] Dennis Cox, *Handbook of Anti-Money Laundering* (Wiley 2014) ch 13.

[111] EU Commission, 'Summary of Responses to the Public Consultation on the Evaluation and Modernisation of the Legal Framework for IPR Enforcement' (2016) 17 <http://ec.europa.eu/DocsRoom/documents/18661> accessed 17 March 2017.

[112] *L'Oréal v eBay* (n 10) [141].

[113] ibid. [142]

[114] *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14* [2016] ECLI:EU:C:2016:689 (CJEU) 96.

1) identify customers or uploaders with a view to be able to enforce against repeat infringers and, depending on the type of platform content, evaluate the infringement risk exposure for the platform.

2) as a deterrence against users to infringe rights.

KYC processes should be flexibly defined according to the type of platform, or content that is being hosted or uploaded. For example, customer identification requirements could be more comprehensive in the area of e-commerce were a contractual relationship is established between the platform and the seller, or where there is deeper integration into the platform, such as use payment or delivery services, or detailed product data upload. By contrast, for user comments on a news portals, user identification criteria could be less onerous taking account of freedom of expression rights. This was confirmed in the *Delfi* judgement where the Court acknowledged the importance of user anonymity for posting comments on internet news portal. At the same time, it acknowledged that different levels of anonymity may be available and appropriate and that they must be balanced against other rights. Those different levels could for example, consist of a registration which is only visible to the ISP but ensures complete anonymity vis-a vis other users[115]. In any case, sectoral KYC obligations should be determined following a thorough balancing exercise with fundamental rights. In parallel to the KYC processes platforms would be obliged to engage in a detailed risk assessment exercise about the susceptibility of their business model and processes to illegal activity and illegal content. The important element here is that that risk assessment process is documented and available to the regulator on request. The criteria for such risk assessment could be derived from existing platform data on infringing use, notice and takedowns, content use and financial data. For example, an ecommerce or digital content platform would need to demonstrate that it is aware of the fact that certain product categories or types of content are more susceptible to infringing use/illegal activity than others. (Ad) revenue, sales and content use/sharing data could be crosschecked with other data gathered through fraud detection activities to assess risks. In a social media setting, context-based user activity, coupled with for example ad revenue statistics could serve as means for the platform to identify activity with higher risk exposure to illegal content or use. All these activities would demonstrate the platform is acting as a responsible and diligent operator. As detailed above, these kind of obligations are not

[115] See for example in: *Delfi AS v Estonia, no 65469/09* (ECtHR (Grand Chamber)). [147] – [149]

new and have been implemented in a number risk regulations, with more recent examples being anti-money laundering and the new GDPR[116].

4.3.2. Risk-based transaction Monitoring

The AML framework prescribes ongoing monitoring of both transactions and the business relationship. The ultimate aim is to spot changes in the risk profile of a customer and to prevent and detect money laundering or terrorist financing activities.

For online platforms, there would be two important ongoing monitoring stages:

1) transaction monitoring during product/content upload;

2) ongoing platform surveillance for infringing activity on the platform[117].

Platforms could be required to establish rules-based systems for high-risk activities and content, e.g. media files highly susceptible to copyright infringement, content highly likely to consist of hate speech or highly regulated product sectors on ecommerce platforms. The ECD already requires that an ISPs must not have "actual knowledge of illegal activity or information and, …, is not aware of facts or circumstances from which the illegal activity or information is apparent"[118] for it to benefit from the liability exception. In *L'Oréa*l, this awareness was related to being a diligent economic operator[119]. Similarly, German courts have asked peer-to-peer and video sharing platforms to check content on their site pre-emptively depending on the availability of effective filter technology and depending on the susceptibility of their business model to infringing uses[120]. The effectiveness and adequacy of technology monitoring for illegal live streams was also discussed in the recent Football Association Premier League case in the UK[121]. Courts have started to consider more routinely the role of filtering systems or other proactive measures in preventing infringing content and activity with regards to hate speech and defamatory content. For example, in the UK Google's ability in light of "existing technology" to block privacy-infringing images

[116] See supra (n 76, n 108)
[117] This may still be possible in order to detect any infringements that may not have been captured during upload, modifications of content online, or when risk profile adjustments require additional sweeps.
[118] ECD (n 2). Article 14 (1)
[119] *L'Oréal v eBay* (n 10) [120].
[120] *Sharehoster II, 5 U 111/08* (2009) openJur 2009, 1105 (OLG Hamburg) [137]; *GEMA v YouTube, 310 O 461/10* (2012) openJur 2012, 36010 (LG Hamburg) [125–127].
[121] *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] 2017 EWHC 480 Ch (England and Wales High Court (Chancery Division)) [52, 64–68].

and its compatibility with Article 15 ECD has been discussed[122]. In Austria and Germany courts have made similar deliberations with regards to hate speech and defamatory content on Facebook[123]. Finally, in *Delfi* the ECHR engaged in a more detailed assessment on the proactive filtering measures and risk assessment activities targeted at preventing illegal hate speech that can be expected of an online news portal[124]. Other emerging case law across EU Member States could be analysed for prevention and filtering obligations with a view to use them for duty of care standards regarding filtering and infringement prevention[125]. In China courts have made platforms' "red flag" knowledge of popular video content, which was more at risk of being infringed, and the deployment of subsequent (risk-based) content filtering subject to duty of care requirements[126]. This is similar to demands made by *Citron et al* in the US, who argue that platforms' "good faith" efforts to proactively identify and restrict abusive content should automatically confer liability onto them under the Communications Decency Act[127].

A duty of care standard in content monitoring would ask platforms to demonstrate that they have performed a risk assessment of possible infringing uses of their platform and assessed and classified the legal risk related to their content. They would then need to demonstrate that they have adapted the use of prevention and filtering measures using a risk-based approach, for example by focussing on the high risk activities identified through their risk assessment. This demonstration could be achieved through a requirement to document and retain their risk assessments and risk ranking.

A methodology for such a risk-based filtering could see a mandatory risk classification of the types of speech or user-generated-content most susceptible to being unlawful. The advantage of a risk based approach to filtering is that it does not require monitoring of the entire platform's content. It would only be directed at activities that correspond to a certain risk profile. The filtering

[122] *Glawischnig-Piesczek, C-18/18* (n 24) [49–54].
[123] In Austria: *Inanspruchnahme des Host-Providers: Entfernung von Hasspostings in sozialen Netzwerken, 5 R 5/17t* [2017] GRUR Int 2017 800 (OLG Wien) [10–11]. In Germany: *Haftung eines sozialen Netzwerkes für durch Dritte hochgeladene ehrverletzende Inhalte, 11 O 2338/16 UVR* [2017] MMR 2017 347 (LG Würzburg).
[124] *Delfi AS v. Estonia, no. 65469/09* (n 105) [62, 122, 129, 155–159].
[125] Leistner (n 31).
[126] Jie Wang, 'Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – As Compared to the US and German Routes' (2015) 46 IIC - International Review of Intellectual Property and Competition Law 275, 284–286.
[127] Citron and Wittes (n 37) 15. Communications Decency Act of 1996 (CDA) s 230(c) (1).

intensity could also vary according to risk profile. In practice, this could mean filtering of content by subject categories, keywords, or other criteria. Some of the approaches listed under Section 3 could be utilized, such as a context based risk classifications in social media[128], paired with specific content flags. If combined with a follow-the-money approach, this could help in sustainably reducing the financially viability of infringers[129].

Platforms and other ISPs are already engaging in these kinds of risk management, filtering and detection activities[130]. These systems are integrated into holistic company risk management activities, such as fraud or payment risks[131], and draw their data from areas across the company (financial/revenue, customer, product, supply chain data)[132]. Mandating a risk-based approach to prevention through transaction monitoring, and setting broad framework conditions for its application could be a way of dragging existing filter algorithms into the light. If platforms were required to explain the risk assessment, the ensuing choice and scope of prevention and filtering technology as well as the operational procedures to regulators, this could create the kind of transparency which is currently needed[133]. That transparency is in danger of being eroded, however, by pushing for self-regulated, industry owned infringement prevention solutions[134].

But even in a co-regulated, technical risk management system there remain accountability and abuse challenges. These complex filtering algorithms will execute on a multitude of embedded normative choices and legal norms which cannot be grasped easily by regulators or users[135]. It will therefore be important to require obligatory, periodic algorithm audits, by which human beings review the technical decisions made by the filtering algorithms, to ensure compliance with legal

[128] Lavi (n 41).

[129] EU Commission, 'Promoting a Fair, Efficient and Competitive European Copyright-Based Economy in the Digital Single Market, COM(2016) 592 Final' 9–10. The follow-the-money approach aims at cutting the revenue stream connected to infringing activities on the internet. Under this, intermediaries such as payment service providers or online advertising services which facilitate revenue generation on websites with illegal content would be brought on board to intercept these activities.

[130] Friedmann (n 24); Wang (n 115). In addition, the activities of YouTube or other platforms on employing content filtering technologies are well known and do not need further elaboration.

[131] Gadinis and Mangels (n 77) 885–886. Demonstrate how AML activities are integrated in wider fraud detection activities of companies.

[132] Ruch and Sackmann (n 76).

[133] Bamberger (n 68).

[134] As discussed in Section 3.2.

[135] Bamberger (n 68) 737–738.

norms and warrant against automation bias and abuse[136]. This review could for example be done by independent auditors or by technically skilled and specialised regulators.

4.3.3. Platform Enforcement and reporting

Under the AML framework, transactions proven or suspected of money laundering or terrorist financing need to be reported to regulatory authorities. Since the fight against money laundering is considered a matter of public interest[137] this appears to be appropriate . Reporting of suspicious transactions on this scale is unlikely to be warranted however around content liability, which in most cases falls under civil law and torts[138]. For example, as stated in *Promusicae*, Member States cannot be obliged to lay down obligations to communicate personal data in civil proceedings related to copyright infringements[139]. Moreover, member states must ensure they apply a balancing exercise with fundamental rights when being confronted with requests for personal data as regards alleged infringers[140].

However, the ability to enforce effectively against infringers remains essential for a well-functioning duty of care standard. This third component of a duty of care regime could therefore be used to define and standardise *ex post* measures that platforms would need to comply with. There could be three distinct elements:

1) Automated takedown conditions: content filtering systems will be designed to take down infringing content automatically. In fact, these systems exist already and they are deployed by a number of platforms[141]. However, it is important for safeguarding of due process and user rights that there are defined and harmonised criteria for automated takedown. These harmonized and standardized criteria would include requirements for contacting affected parties (e.g. timing, message content) and the modalities for counter claims.

---

[136] ibid.

[137] DIirective (EU) 2015/849 (n 6). Recital 42, Article 43

[138] Counterfeiting in e-commerce could be an exception, as this may be linked to organized crime or anti-money laundering. Where this is the case a duty of care standard could include a reporting requirement to that effect in very limited circumstances and under a strict balancing exercise.

[139] *Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06* [2008] ECLI:EU:C:2008:54 (CJEU) [58–60].

[140] ibid 66–68.

[141] A cases in point is Google's ContentID filtering software. 'How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en> accessed 28 September 2017.

2) Notice and Takedown (NTD) criteria: NTD relies on third parties, such as users, authorities or rightsholders, to inform platforms of allegedly infringing content. Under current EU law the ISP would need to remove expeditiously infringing content of which it has been notified[142]. However, the ECD does not set any more detailed or harmonised criteria for NTD. The EU Commission is currently reviewing whether there is a need for Europe-wide NTD processes[143]. In its public consultation on online platforms 70% of respondents argued for sector specific NTD regimes[144]. Typical criteria that could be defined in such a standard are: notification modalities (e.g. the technical means – web forms, email; who can send it); notice content (e.g. the detail of information provided, declarations of perjury etc.); processing modalities (e.g. maximum handling time, platform information to notice providers and other stakeholders); counter notice requirements.

3) Reporting: compliance reporting requirements are standard in many legal areas, including in AML[145]. In complex technical environments reporting may make it easier to demonstrate compliance in an understandable way to the public, regulator or political representatives[146]. However, mandatory compliance reporting also has the additional value of reducing conflicts of interest and fostering a compliance culture within the company. These effects will be enhanced when coupled with the promise of immunity[147]. The duty of care reporting requirements could include data on the number of: takedowns (automated and notified) in any desired detail, counter claims and their success rate, user accounts suspended or other sanctions, actions against repeat infringers. Whether these metrics are public or shared between industry and regulator would need to be subject to the type of content and the public interest involved. This could for example replace or supplement the rather exclusive information sharing requirements between rightsholders and platforms proposed in the recent Copyright Directive proposal[148]. By contrast, the recent

[142] ECD (n 2).
[143] EU Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe COM(2016) 288 Final' 9.
[144] EU Commission, 'Synopsis Report on the Public Consultation on the Regulatory Environment For Platforms, Online Intermediaries and the Collaborative Economy' 17 <https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and> accessed 29 March 2017.
[145] In the EU statutory reporting requirements are imposed by the REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals), health and safety regulation, labour law, tax law and for statistical purposes, to name but a few.
[146] Cohen (n 54) 406.
[147] Gadinis and Mangels (n 77).
[148] Copyright Directive Proposal (n 25). Recital 38

Commission communication on tackling illegal content on the internet, which encourages standardized notice and takedown transparency reporting [149] is a useful step in the right direction.

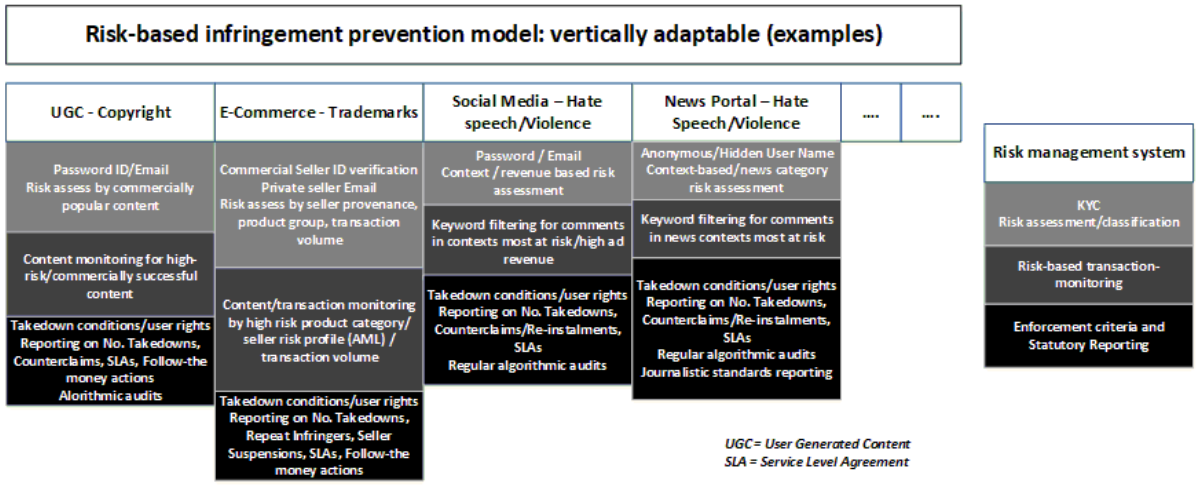

Figure 1

4.4. Limitations and risks

There are also limitations to the proposed duty of care standard which should be mentioned. For one, standardization is initially a time-consuming process and technology and market developments may over-run it. However, once in place the advantage of the solution proposed here is that it is adaptable. Secondly, co-regulatory solutions could also lead to a lack of procedural legitimacy if highly technical industry and regulator groups work in exclusive circles whereby the former set the tone and direction of the standard setting process due to their intimate technical knowledge[150]. A possibly remedy proposed in this article would consist of mandatory, regular reporting and external audits in order to make the standard developments process transparent and accountable. Lastly, there also competition concerns if the standard setting is dominated by leading platforms, hindering new market entrants to prosper.[151]. Elevating existing technical risk management systems for infringement prevention, developed by leading platforms, to a state-of-the art standard for the entire sector could pose high entry barriers for new, small ISPs. It has been

[149] EU Commission, 'Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms, COM(2017) 555 Final' (n 3) 16.
[150] Marsden (n 7) 4.
[151] Cohen (n 54) 395. A process called "deep capture"

argued that, if smaller players were forced to adopt or compete with Google (YouTube) or Facebook's existing technologies for identifying e.g. copyright infringing or hate speech content, they would not be able to enter the market[152]. A possible strategy could involve designing "sandbox" approaches to the use of filtering technology. Regulatory sandboxes are considered in highly innovative and fast-moving sectors of industries subject to more complex and technical regulatory requirements[153]. According to this, smaller, innovative market entrants are exempt from the more onerous regulatory provisions of established market players. They would be allowed to develop and test their products or services with a view to exploring the impact of regulation[154]. An example is the recent German law obliging social media companies to identify and takedown hate speech[155].

5. Conclusion

This paper demonstrated that there is an emerging opinion that new, normative duties of care, could be a way forward to involving platforms consistently in efforts to prevent and remove infringing content online. These duties of care should be adaptable to the type of content or platform design. While the borders between protectable "passive" and liable "active" intermediaries are disappearing in practice, Article 15 ECD could be seen as a formidable obstacle to formulating more proactive infringement prevention rules. However, this paper also tried to demonstrate that the justifications for Article 15, which dates back to the early days of the internet economy were motivated by a desire to protect a nascent industry. These economic justifications may be outdated today as the platform economy has come of age. Moreover, courts can perform effective balancing exercises between rights protection of online content and fundamental rights of users/uploaders without the use of Article 15. Meanwhile, the term "general monitoring" is too

[152] See for example: Nolte and Wimmers (n 24) 22–23., 'Copyright Reform: Open Letter from European Research Centres' (24 February 2017) <http://bit.ly/2loFISF> accessed 3 March 2017.

[153] A more detailed discussion of the application of the a regulatory sandbox approach in the Fintech sector can be found at: Dirk A Zetzsche and others, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 2017 University of Luxembourg Law Working Paper <https://ssrn.com/abstract=3018534> accessed 8 January 2018.

[154] EU Commission, 'Fintech: A More Competitive and Innovative European Financial Sector, Consultation Document' 16–17 <https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf> accessed 9 January 2018.

[155] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken 2017 (BGBl I S 3352 (Nr 61)). Article 1, Para 1, Section 2. This law exempts social networks with less than 2 million domestic users from key reporting and duty of care requirements relating to identifying and removing infringing content requirements.

unspecific to be applied in a meaningful way to today's platform risk management systems. Notwithstanding this, there are various proposals both from academia and the EU to create duty of care style infringement prevention obligations. Most of these relate to specific content sectors or platform designs. They are a mixed bag of self and co-regulatory measures, and not all proposals appear to consciously select a certain type of governance model. The EU Commission has currently opted for self-regulatory solutions. Whether this is the best choice is questionable. While there is a natural drift for self-regulatory solutions in highly technical, fast moving and innovative sectors, they have major drawbacks, such as democratic legitimacy and automation bias influenced by commercial interest scope creep and self-referentiality. This paper suggests that a co-regulatory model, by which industry and regulators are mandated to create risk management standards is a better way forward. The current AML framework is presented as a possible model for designing such a duty of care standard. There are notable similarities in the financial transaction and online content management sectors which lend themselves to this analogy. The duty of care standard for preventing infringing content could be structured along the current AML framework. It would impose three elements: KYC, content monitoring, and enforcement and reporting obligations. The standard would follow a risk-based approach, asking platforms to engage in transparent and auditable risk assessments of their business model and content following a mandated risk management framework. These frameworks could be adapted to different sectors, depending on type of content or platform design. Depending on the risk classification, platforms would then need to implement processes which effectively address the risks. Platforms would be given freer choice regarding the operational and technological means with which they address these risks. Finally, harmonised NTD procedures could be part of the enforcement component of such a standard. Transparency and democratic accountability of such a standard would be safeguarded by regulator involvement in the standard setting process, and regular compliance reporting and external audit requirements.

Bibliography

Secondary Sources

Ai L and Tang J, 'Risk-based Approach for Designing Enterprise-wide AML Information System Solution' (2011) 18 Journal of Financial Crime 268

Angelopoulos C, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International BV 2017)

Bamberger KA, 'Technologies of Compliance: Risk and Regulation in a Digital Age' (2009) 88 Tex. L. Rev. 669

Bergström M, Svedberg Helgesson K and Mörth U, 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management' (2011) 49 JCMS: Journal of Common Market Studies 1043

Büllesbach A (ed), *Concise European IT Law* (2nd ed, Kluwer Law International ; Sold and distributed in North, Central and South America by Aspen Publishers 2010)

CapGemini and BNP Paribas, 'World Payments Report 2017. A Preview into the Global Payments Landscape.' (2017)

Citron DK and Wittes B, 'The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity' (2017) University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2017-22 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007720> accessed 18 September 2017

Cohen JE, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369

Cole MD and Quintel T, '"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)', *Comparative Perspectives on Privacy in an Internet Era*, vol VII (CAP Forthcoming)

Cox D, *Handbook of Anti-Money Laundering* (Wiley 2014)

Domo.com, 'Data Never Sleeps 4.0 - 2016 Data' <https://web-assets.domo.com/blog/wp-content/uploads/2016/06/16_domo_data-never-sleeps-4-2.png> accessed 30 April 2018

Edwards L and Veale M, 'Slave to the Algorithm? Why a "Right to Explanation"Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18

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

——, 'Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document , SEC(2011) 1641 Final'

——, 'Synopsis Report on the Public Consultation on the Regulatory Environment For Platforms, Online Intermediaries and the Collaborative Economy' <https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and> accessed 29 March 2017

——, 'Commission Updates EU Audiovisual Rules and Presents Targeted Approach to Online Platforms, IP/16/1873' <http://europa.eu/rapid/press-release_IP-16-1873_en.htm> accessed 22 December 2017

——, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe COM(2016) 288 Final'

——, 'Promoting a Fair, Efficient and Competitive European Copyright-Based Economy in the Digital Single Market, COM(2016) 592 Final'

——, 'Summary of Responses to the Public Consultation on the Evaluation and Modernisation of the Legal Framework for IPR Enforcement' (2016) <http://ec.europa.eu/DocsRoom/documents/18661> accessed 17 March 2017

——, 'Fintech: A More Competitive and Innovative European Financial Sector, Consultation Document' <https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf> accessed 9 January 2018

——, 'Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms, COM(2017) 555 Final'

——, 'Next Steps against Fake News: Commission Sets up High-Level Expert Group and Launches Public Consultations, IP/17/4481' <http://europa.eu/rapid/press-release_IP-17-4481_en.htm> accessed 22 December 2017

'European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech' <http://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 9 March 2017

'FATF - Members and Observers' <http://www.fatf-gafi.org/about/membersandobservers/> accessed 22 September 2017

'FATF Countries' <http://www.fatf-gafi.org/countries/> accessed 25 September 2017

'FATF Recommendations 2012 - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 22 September 2017

Freeman J, 'Consumer Legislation and E-Commerce Challenges' (2015) 2 Rivista Italiana di Antitrust/Italian Antitrust Review <http://iar.agcm.it/article/view/11380> accessed 19 September 2017

Friedmann D, 'Sinking the Safe Harbour with the Legal Certainty of Strict Liability in Sight' (2014) 9 Journal of Intellectual Property Law & Practice 148

Frosio GF, 'The Death of No Monitoring Obligations' (2017) 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 199

Gadinis S and Mangels C, 'Collaborative Gatekeepers' (2016) 73 Wash. & Lee L. Rev. 797

Gao S and others, 'Knowledge-based Anti-money Laundering: A Software Agent Bank Application' (2009) 13 Journal of Knowledge Management 63

Helberger N, Kleinen-von Königslöw K and van der Noll R, 'Regulating the New Information Intermediaries as Gatekeepers of Information Diversity' (2015) 17 info 50

Helman L and Parchomovsky G, 'The Best Available Technology Standard' [2011] Columbia Law Review 1194

'How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en> accessed 28 September 2017

Husovec M, 'Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13' <http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/> accessed 28 September 2017

Kerber W and Wendel J, 'Regulatory Networks, Legal Federalism, and Multi-Level Regulatory Systems' (2016) 13–2016 <http://ssrn.com/abstract=2773548> accessed 6 April 2017

Lavi M, 'Content Providers' Secondary Liability: A Social Network Perspective' (2015) 26 Fordham Intell. Prop. Media & Ent. LJ 855

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

Ligeti K and Lassalle M, 'La Quatrième Directive Anti-Blanchiment: Quels Changements Pour Le Luxembourg?' (2016) 2 Revue luxembourgeoise de bancassurfinance

Lodder AR and Murray AD (eds), *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing 2017)

Marsden CT, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011)

Martinez Mata Y, 'Bolkestein Revisited in the Era of the Sharing Economy' [2017] Revista Electrónica de Estudios Internacionales <http://www.reei.org/index.php/revista/num33/notas/bolkestein-revisited-in-the-era-of-the-sharing-economy> accessed 12 September 2017

'Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet, 2011'

Nolte G and Wimmers J, 'Wer Stört? Gedanken Zur Haftung von Intermediären Im Internet – von Praktischer Konkordanz, Richtigen Anreizen Und Offenen Fragen' (2014) 16 GRUR

Pasquale F, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487

Richardson JB, 'With Great Power Comes Little Responsibility: The Role of Online Payment Service Providers with Regards to Websites Selling Counterfeit Goods' (2014) 12 Canadian Journal of Law and Technology <https://ojs.library.dal.ca/CJLT/article/view/6607> accessed 20 March 2017

Ruch M and Sackmann S, 'Customer-Specific Transaction Risk Management in E-Commerce', *Value creation in e-business management* (Springer 2009)

Saurwein F, Just N and Latzer M, 'Governance of Algorithms: Options and Limitations' (2015) 17 info 35

Schultz J, 'The Amount of Data Created Each Day on the Internet in 2017' <https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/#> accessed 30 April 2017

Senden LAJ and others, *Mapping Self-and Co-Regulation Approaches in the EU Context'': Explorative Study for the European Commission, DG Connect* (European Commission 2015) <http://dspace.library.uu.nl/handle/1874/327305> accessed 10 March 2017

Spindler G, Schuster F and Anton K (eds), *Recht Der Elektronischen Medien: Kommentar* (2 Aufl, CH Beck 2011)

Spindler G and Thorun C, 'Die Rolle Der Ko-Regulierung in Der Informationsgesellschaft' (2016) 6 MMR-Beil. 1

Stalla-Bourdillon S, 'Internet Intermediaries As Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well.', *The responsibilities of online service providers* (Springer Berlin Heidelberg 2016) <http://link.springer.com/10.1007/s11948-015-9734-1> accessed 17 February 2017

Sylvain O, 'Intermediary Design Duties' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997141> accessed 19 September 2017

Thompson E, 'Money Laundering Watchdog Scrutinizes Facebook, Social Media' (2017) <http://www.cbc.ca/news/politics/facebook-twitter-privacy-moneylaundering-1.4020638> accessed 30 April 2018

Valcke P, Kuczerawy A and Ombelet P-J, 'Did the Romans Get It Right? What Delfi, Google, EBay, and UPC TeleKabel Wien Have in Common', *The responsibilities of online service providers* (Springer Berlin Heidelberg 2017)

Verbiest T and others, 'Study on the Liability of Internet Intermediaries, Markt 2006/09/E'

Waisman A and Hevia M, 'Waismann Theoretical Foundations of Search Engine Liability' (2011) 42 International Review of Intellectual Property and Competition Law 785

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

Weinbaum C, 'Covert Influence Is the New Money Laundering' (2017) <https://techcrunch.com/2017/11/05/covert-influence-is-the-new-money-laundering/> accessed 30 April 2018

Yasaka N, 'Data Mining in Anti-Money Laundering Field' (2017) 20 Journal of Money Laundering Control 301

Zetzsche DA and others, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 2017 University of Luxembourg Law Working Paper <https://ssrn.com/abstract=3018534> accessed 8 January 2018

'Copyright Reform: Open Letter from European Research Centres' (24 February 2017) <http://bit.ly/2loFISF> accessed 3 March 2017

Case Law

Asociación Profesional Élite Taxi v Uber Systems Spain SL, C-434/15 [2017] ECLI:EU:C:2017:981 (CJEU)

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, C-360/10 [2012] ECLI:EU:C:2012:85 (CJEU)

CG v Facebook Ireland Ltd & Anor [2016] 2016 NICA 54 (Court of Appeal in Northern Ireland)

Delfi AS v Estonia, no 65469/09 (ECtHR (Grand Chamber))

GEMA v YouTube, 310 O 461/10 (2012) openJur 2012, 36010 (LG Hamburg)

Glawischnig-Piesczek, C-18/18 (CJEU)

Glawischnig-Piesczek, v Facebook, 6Ob116/17b (Oberster Gerichtshof, Republik Österreich)

Haftung eines sozialen Netzwerkes für durch Dritte hochgeladene ehrverletzende Inhalte, 11 O 2338/16 UVR [2017] MMR 2017 347 (LG Würzburg)

Inanspruchnahme des Host-Providers: Entfernung von Hasspostings in sozialen Netzwerken, 5 R 5/17t [2017] GRUR Int 2017 800 (OLG Wien)

L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd and others, C-324/09 [2011] ECLI:EU:C:2011:474 (CJEU)

Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06 [2008] ECLI:EU:C:2008:54 (CJEU)

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (Scarlet Extended), C-70/10 [2011] ECLI:EU:C:2011:771 (CJEU)

Sharehoster II, 5 U 111/08 (2009) openJur 2009, 1105 (OLG Hamburg)

The Football Association Premier League Ltd v British Telecommunications Plc & Ors [2017] 2017 EWHC 480 Ch (England and Wales High Court (Chancery Division))

Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14 [2016] ECLI:EU:C:2016:689 (CJEU)

Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14 [2016] ECLI:EU:C:2016:689 (CJEU)

Statutes and Draft Statutes

Communications Decency Act of 1996 (CDA)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 187 2000

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 2004

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing 2005

Directive 2015/849/EU of the European parliament anf of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing 2015

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 2015

Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken 2017 (BGBl I S 3352 (Nr 61))

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final 2016

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, COM(2016) 450 final 2016

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market, COM(2016) 593 final 2016

Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC 2017