Content 'responsibility':

The looming cloud of uncertainty for internet intermediaries.

By Dr. Monica Horten,
For the Center for Democracy and Technology

September 2016

CENTER FOR DEMOCRACY & TECHNOLOGY

About the Author

Dr. Monica Horten is a Visiting Fellow, London School of Economics and Political Science. She currently serves as a Council of Europe expert on the Programmatic Co-operation Framework for Ukraine, Moldova, and Georgia, and she previously sat on the Committee of Experts on Cross-border Flow of Internet Traffic and Internet Freedom.

She is the author of several academic papers and three books on internet policy issues: *The Closing of the Net*, *A Copyright Masquerade*, and *The Copyright Enforcement Enigma: Internet politics and the Telecoms Package*.

She has formerly been a telecoms journalist and writes the Iptegrity blog.

TABLE OF CONTENTS

Executive Summary

This paper addresses the topic of intermediary liability in the context of new European Union policy proposals. These proposals introduce a new notion of 'content responsibility'. The paper seeks to understand this notion and its consequences by analysing the policy proposals that have been tabled in 2016, as well as national and European case law.

Section 2 of the paper contains an overview of the current position regarding liability through the lens of copyright. Until now, copyright enforcement has been the major reason for requests to remove or block content. The paper finds that innovative services frequently butt up against existing legal boundaries as developers seek to innovate. The technological complexity of some liability claims can lead to decisions that overlook the positive externalities for society as a whole.

Section 3 discusses the current case law in the EU. The law calls for any restrictions on content to be targeted and narrow in scope. Broad injunctions for preventative action or stay down would be incompatible with the E-Commerce Directive[1]. Any restrictive measures must comply with the principles laid down in the European Convention on Human Rights (ECHR) Article 10.2, namely that they should be prescribed by law, fulfill a legitimate aim and a pressing social need, and be specific to the issue being addressed.

Section 4 analyses the proposals on the table in 2016 (see Annexe). It argues that the proposals entail a scaling up of liability into three new policy areas: counter-terrorism, hate speech, and protection of minors. The Terrorism Directive currently being processed in the European Parliament seeks the removal of content 'glorifying terrorism' from social media and other websites. The paper considers issues that are not addressed in the Directive, such as the possibility for judicial review of such measures. The proposed Audio-Visual Media Services Directive seeks to make video-sharing platforms monitor and remove perceived hate speech, as well as content that may "impair the physical, mental or moral development of children". The paper argues that the definitions for both measures are overly broad, and that compliance would mean monitoring and suppression of links and manipulation of search algorithms. Intellectual property rights (IPR) enforcement proposals expected this autumn may introduce a follow-the-money approach, and the paper highlights that while this appears straightforward, it could in fact lead to false positives.

This is followed by a more in-depth discussion in Section 5 of the issues raised by these proposals. The paper argues that the proposals, taken together, could imply the equivalent of an obligation to monitor. It highlights concerns raised by self- or co-regulatory responses, especially in light of the technological complexity of the decisions that will have to be taken. As a consequence of the proposed measures, intermediaries face increasing legal uncertainty with potential negative economic consequences.

The paper concludes that the proposed measures should be balanced against the economic policy aims in the Digital Single Market strategy, and the duty of the European Commission and Member State governments to guarantee the right to freedom of expression under the European Convention on Human Rights.

The paper makes the following recommendations for future EU policy in this area:

EU policy makers should safeguard the internet as an open, innovative, and vibrant platform for the exercise of users' free expression and other fundamental rights. Any policy measures adopted to restrict content online should be compatible with the E-commerce Directive and guarantee safeguards as established under Article 10 of the European Convention on Human Rights. This includes any self- or co-regulatory measures implemented to fulfil a State policy aim.

Policy makers should strengthen liability protection for intermediaries, and positively confirm that any form of general monitoring is not lawful.

No attempts should be made to create new categories of intermediaries, such as active hosting. This would result in a narrowing of the activities of intermediaries that are covered by existing liability protections. It would lead to increased legal uncertainty and cost for internet-based start-up companies. It would limit the scope for users to upload and engage with online content, with negative consequences for free expression.

Policy makers should refrain from creating new categories of rights in online content, such as ancillary rights for publishers. Such measures would have a negative impact on free expression, and on internet-based innovation and entrepreneurship.

Any restrictive measures must be carefully targeted towards content that is clearly illegal; there must be full judicial oversight and transparency as to the type and volume of content

that is targeted, as well as the duration and territorial scope and the type of restriction implemented. There must be compliance with the principles of necessity, proportionality, and foreseability, and such measures should go no further than is essential to address the social need pursued. Due process must be in place that allows appeal of wrongful take downs or blocking decisions.

While the protections in the E-Commerce Directive should be maintained and reinforced, the Commission might consider whether **notice-and-action procedures could be improved and more consistently implemented across Member States.**

Introduction

A file-hosting company had its online payments account shut down because it refused to monitor user traffic for illegal content.

Music DJs sharing legal music mixes found their tracks had been removed without explanation.

A web-hosting company heard via the media that its client's website had been blocked under terrorism law.

These are three instances where liability for internet content ceases to be an abstract concept and touches the reality of business and cultural life. They illustrate how the pressure being placed on internet intermediaries to 'remove' illegal content is rippling down into the smallest corners of the online world.

Internet intermediaries are the companies that provide the hosting, storage, and transmission of user-generated content and that enable access and retrieval of this content by the author and other users. Intermediaries include social media sites, video or photo sharing platforms, applications, broadband providers, cloud services, file and web hosting companies, search engines, and others. Intermediaries are pivotal in the functioning of the internet and they have enabled the development and growth of many services that we enjoy online.

Moreover, the role of intermediaries in protecting free speech and encouraging civic engagement[2] is widely recognised. Conversely, it is recognised that the imposition of content restriction obligations on intermediaries is a form of censorship.[3]

The notion of liability in this context deals with the likelihood of intermediaries being sued for damages, issued injunctions, or otherwise charged over illegal content that is created, up or downloaded, stored, or distributed on their system. 'Illegal' may mean that the content breaches criminal law, such as child sex abuse images or videos that incite imminent criminal or terrorist acts, where the speaker of the content could face fines or a jail sentence. 'Illegal' may also mean that the content infringes on civil law – for example copyright – and the individual who posted it may incur damages, or face a demand for royalty payment. Alternatively, they could receive an injunction whereby they could be asked to stop the infringing activity through restrictive methods such as blocking, filtering, or suspending accounts.

The freedom of intermediaries to provide services without fear of damaging lawsuits or heavy penalties has been an important factor in enabling free expression, innovation, and commerce. Currently, EU policy incorporates a balance that protects intermediaries from such liabilities, while enabling third parties to request limited and targeted action against clearly illegal content. Importantly, EU regulation prohibits any kind of 'general obligation to monitor' being imposed.

But is that balance about to be tipped over? The European Commission is putting forward a raft of proposals under the Digital Single Market initiative[4] (see Annexe) that target internet intermediaries. These proposals have been reframed as 'responsibility for content' rather than 'liability'. They are the result of pressure from many third-party interests, such as law enforcement, civil society groups, and the entertainment industries, to mandate more 'responsible behaviour' among intermediaries. They seek to impose various forms of content restrictions to support policy aims such as fighting terrorism, limiting the spread of hate speech, and protecting minors online.

The questions for this paper are to understand what such 'responsible behaviour' might be, and the possible consequences of mandating it under law. The paper examines current copyright enforcement case law to obtain a perspective on how liability impacts intermediaries. It then outlines the current scope of EU law regarding intermediary liability, before moving on to analysing the new EU proposals and their potential impact.

Liability Perspectives Through the Lens of Copyright

Until now, copyright enforcement has been the major content liability issue for internet intermediaries in the European Union. Requests for copyright content removal or blocking outnumber all others. For example, transparency reports from Google reveal 86 million copyright takedown requests per month,

with just over 9 million from the British recorded music industry alone.[5] Blocking orders can entail lists of several thousand URLs. Over the past decade, a growing body of case law has developed, providing a medium- to long-term perspective on how liability may affect intermediaries. Through the lens of copyright, we can explore notions such as "duty of care" and the impact of lengthy litigation processes. This analysis is less concerned with a strict legal interpretation of the definition of infringement than with the consequences for the intermediary's business and for the wider society.

The impact of litigation

Copyright litigation poses a significant risk to intermediary businesses. Legal proceedings are a major cost imposed by an uncertain liability regime, as identified in a study by Oxera.[6] Lengthy legal proceedings can become a drain on resources and funds, leading ultimately to the risk of bankruptcy and closure of the business. In the copyright litigation context, there is a familiar pattern of litigation being used to wear down intermediaries' resistance to measures that rightholders seek to impose, such as blocking or deactivating accounts.

Take for example the case of Netlog[7], a popular Belgian social media platform. By the beginning of 2009, it had grown with seed funding to 56 million users who uploaded videos, music, and other content to their profiles, which they shared with others on the site. It was hailed as a European success story. In 2009, Netlog was sued by the Belgian collecting society SABAM and threatened with an obligation to proactively filter user-uploaded content for potential copyright infringements. Netlog argued that this obligation was a general obligation to monitor, which is unlawful under EU law. In 2012, it won a ruling from the European Court of Justice. The ruling came as Netlog was losing users to Facebook. Despite the win, its parent company was sold in December 2012 for just $25 million and is now part of the US-controlled InterActiveCorp. In December 2014, Netlog vanished from the internet.

Another example is SoundCloud, the Swedish-owned, Berlin-based hosting service for DJs and the artist community, which has 175 million monthly active listeners. After five years of unsuccessful negotiations for licence fees, it was sued by the music-licensing society PRS in August 2015. In 2015, around the same time as the PRS lawsuit, SoundCloud's professional users began to complain about copyright-based removal of their mixes and tracks, including tracks to which they owned the rights. A radio station, Radar Radio, had its account suspended.[8] By December 2015, the litigation was dropped and SoundCloud and PRS reached an agreement for the multi-territory licencing of PRS repertoire.[9]

Other intermediaries face litigation threats over royalties. YouTube has been hit with several lawsuits in France and Germany. It fought a 7-year court battle with the German music collecting society GEMA over copyright royalties. At issue was the fee per stream of GEMA-licensed songs. GEMA claimed that royalties were owed for music videos posted on YouTube. The latter refused to pay, claiming that GEMA demanded too high a payment. In January 2016, the Munich High Court determined that YouTube was neither directly nor indirectly liable for copyrighted content uploaded onto its platform. The two litigants subsequently held out-of-court discussions.

Spotify is the successful, legal music streaming service co-owned by the music labels, but even it has had difficulties. When its service launched in Germany in 2012, Spotify had not been able to reach an agreement with GEMA. The two are still arguing with each other.[10]

These cases raise critical business issues. Rightholders claim there is a 'value gap'. Essentially, they believe they are not being paid enough for users' digital access to their content. But intermediaries can face difficulties in dealing with rightholders. For example, some intermediaries complain that rightholder organisations and collecting societies cannot identify what repertoire they represent.[11] Rightholders are currently demanding that policy makers intervene to address the so-called 'value gap' and this issue appears on the European Commission's policy agenda. It is not at all clear, however, that this is an issue requiring intervention from the Commission. In particular, the EU has already legislated to regulate collecting societies in the Directive on Collective Rights Management[12], which was designed to address the underlying administrative issues within collecting societies.

Ancillary copyright: Unintended consequences for publishers

Demand for royalties by newspaper publishers has, arguably, resulted in direct harms to their business. The large newspaper publishers have been struggling with news aggregators that collate links to news stories. Aggregators offer a new way to access current affairs and send new audiences to traditional media outlets. However, large newspaper publishers claim that search engines benefit from their content but fail to remunerate them for lost audiences and advertising revenue. Publishers have called on search companies to pay licence fees for the including snippets of text from articles that are linked via

their search listings. In some Member States, the publishers succeeded in getting government support for this type of proposal.

For example, in Germany, the Leistungsschutzrecht für Presseverleger (LSR) implemented an 'ancillary copyright' for snippets, allowing publishers to claim royalties from news and content aggregators. However, this law, the so-called "Google tax", has had the opposite of the desired effect. Google, and other online news portals such as T-Online, reacted by ceasing to link to the newspaper publishers' sites in their listings. The publishers found that their website traffic dropped significantly; eventually, they asked for links to be re-instated, without demanding any payment.[13]

In Spain, the large newspaper publishers had lobbied, via their trade body, the Asociación de Editores de Diarios Españoles (Association of Publishers of Spanish Newspapers), for a similar amendment to Spanish copyright law. The amendment introduced a fee to be paid to publishers by online news aggregators for linking to publishers' content and displaying snippets of text from the original article.[14] In November 2014, the law was adopted and the fee became mandatory, such that publishers were not given the option to waive the fee and allow their content to be linked for free if they so wished.

This law resulted in the well-publicised closure of Google News Spain. Spanish content aggregators had to either change their business model or close. The law created uncertainty across the intermediary industry with consequent impact on investment decisions. It reduced consumer choice as smaller periodical publishers suffered. A study for the Asociación Española de Editoriales de Publicaciones Periódicas (Spanish Association of Publishers of Periodical Publications) found that audiences dropped, with a measurable 14% reduction in traffic to publishers' websites.[15] This had an immediate impact on advertising revenues, which are based on audience size. It was estimated that, due to the law, the publishers stood to lose an aggregate of €10 million annually in profits. Small publishers also found the snippets fee to be a barrier to entry.[16] As a consequence, the law favoured a concentration of power in the hands of the large publishers and reduced media pluralism.

Hence, far from being a revenue generator, this "tax" has proven to be a force for market consolidation and loss of audiences. This sort of ancillary copyright proposal is harmful for both media and intermediary industries.

Duty of care: How onerous?

Cloud computing companies and, in particular, file hosting services, are often a target for copyright enforcement litigation on the basis that their users may be uploading, storing, and downloading infringing files. Cloud providers argue that liability for copyright would be an onerous obligation that could have the unintended consequence of hurting users and businesses who use these services for legitimate purposes.[17]

The case of the German file hosting company Rapidshare illustrates how the courts have wrestled with this issue. Rapidshare was once in the top 20 most-visited internet sites. It was subjected to a series of copyright lawsuits from rightsholders from 2007-2012. In 2010, Rapidshare was sued by Atari over a computer game called "Alone in the Dark". From what can be ascertained, Rapidshare had co-operated with rightholders notifications to remove allegedly infringing content. However, Atari argued that Rapidshare had a 'duty' to automatically take preventive action. It demanded that Rapidshare filter the content by keyword and delete all files relating to certain keywords. Rapidshare countered that the filtering demand was taking the notion of a 'duty' too far and would result in files containing legal content being taken down.

In 2011, the Higher Regional Court of Düsseldorf ruled in favour of Rapidshare[18], stating that keyword filtering would be an arbitrary measure since the presence of a keyword is no guarantee that the file includes infringing content, and that requiring a manual check of files was too onerous. However, in 2012, the Bundesgerichtshof (German Federal Court) subsequently overturned the ruling, saying that file-hosters could be asked to take all technically and economically reasonable precautions to prevent the content from becoming available again on its servers.[19] Rapidshare then closed its service to consumers and began offering business-to-business services only. It ceased trading in 2014.

However, when the German government tried to legislate a similar duty of care on file-hosting services to police content, German industry protested and successfully got the draft provision deleted.[20] The industry argued that not only was the provision incompatible with the E-Commerce Directive, but it would have risked criminalising cloud services and social media, and was not economically feasible.

"Störerhaftung" silenced public Wi-Fi

Another German case illustrates the way in which a minor copyright enforcement lawsuit created a national chilling effect.[21]

The central issue was the "Störerhaftung", a form of indirect liability in which a company who has not itself committed an infringement is considered to have contributed in some way towards it.[22] Rightholders have also referred to it as a 'duty of care'.

In May 2010, in the case known as 'Sommer Unseres Lebens'[23], a householder accused of permitting a third party to download a copyright-protected music track was ordered by the Bundesgerichthof (German Federal Court) to password-protect their Wi-Fi. This order was intended to protect the householder against future copyright-infringing activities by family members and guests.

In the context of that individual ruling, the order may have seemed reasonable. However, rightsholders pursued further cases along these lines and the outcome was that many bars, cafes, and other public Wi-Fi owners subsequently closed their Wi-Fi rather than risk liability for maintaining a non-password protected system or being held liable for infringing activity of their customers. Some businesses circumvented the liability risk by outsourcing their Wi-Fi services to a network provider, because network providers were not subject to the Störerhaftung. However, the fact remains that Germany's public Wi-Fi is limited. According to the German industry association eco, there were 996,800 Wi-Fi hotspots in Germany but only a tiny number – around 15,000 – are open.[24] By contrast, South Korea and the UK both have over 180,000 open wireless hotspots.

The Störerhaftung was revoked in 2016 by the German government after the European Court of Justice, in the case of McFadden v Sony, ruled that the Störerhaftung was incompatible with the E-Commerce Directive.[25] German industry was delighted, saying that this change would bring greater certainty for wireless hotspot operators and would have positive effects on the economy.[26]

The unintended consequences of intermediary liability

Critically, the McFadden v Sony ruling stated that in restricting access to lawful communications, the '"Störerhaftung" also restricted freedom of expression and added that, *"Wi-Fi access points indisputably offer great potential for innovation. Any measures that could hinder the development of that activity should therefore be very carefully examined with reference to their potential benefits."*

This statement points to the difficulties in determining issues of policy in complex technology cases. Innovative services frequently butt up against existing legal boundaries as developers seek to create new ways of doing things. A narrow interpretation of the law may find an infringement and overlook the positive externalities. The unintended consequences of some decisions to support copyright enforcement may quash innovation that could bring wider societal benefits. For example, the previously mentioned case regarding open access public Wi-Fi highlights the way that a legal decision failed to take into account the tangible benefits of the technology, which is used for mobile infill in places where there is either no or low mobile coverage and is widely regarded as an essential utility for travellers and tourists. In national emergencies, such as the 2016 Brussels attacks, the authorities rely on it to facilitate access to communications. Notably, the Belgian deputy prime minister, Alexander de Croos, took to the social media platform Twitter to ask people to use Wi-Fi on their mobile devices and avoid making voice calls that could overload the cellular networks.[27] [28]

A red flag is raised here about the danger to innovation. All of the above examples illustrate threats to intermediaries from liability claims and the complexity of some of the rulings. If the decision-making is taken away from the courts and handed to a self- or co-regulatory agreement, as will be discussed later in this paper, the complex systhesis of technological and legal reasoning will not be undertaken.

Current EU Policy: Narrow Scope for Restrictions

EU law on intermediary liability is established under the E-Commerce Directive. This directive enables intermediaries to grow their business, and at the same time, protects the free speech rights of citizens. It does so by incorporating protection for intermediaries who transmit or host content against the possibility that their services are misused by third parties to post or access illegal content.

The law differentiates between two types of intermediaries: network intermediaries and hosting intermediaries. Network intermediaries are 'mere conduits' that transmit the content irrespective of what it is. Network intermediaries are neither directly nor indirectly liable for illegal content; any infringement or offence is the responsibility of the user, and the intermediary is legally protected from being sued or sanctioned.

Hosting intermediaries are similarly protected from liability, provided that they expeditiously remove illegal content when they are provided with actual knowledge that it exists on their site, server, or system.[29] There is a legal debate as to what constitutes 'actual knowledge'. In *RTI v Yahoo!*,[30] the Milan court

said that 'actual knowledge' means a detailed notification incorporating specific URLs; this principle is followed by other national courts.

Importantly, intermediaries may not be given a 'general obligation to monitor'. Hence, the European Court of Justice has ruled that a requirement of continuous monitoring or preventive action by an intermediary is not compatible with EU law. Based on the rulings in *Scarlet Extended* and *Sabam v Netlog*, this principle applies for both hosting and network intermediaries. In the Netlog ruling, the ECJ said that EU law precludes a hosting service provider being required to:

'install a system for filtering information which is stored on its servers by its service users; which applies indiscriminately to all of those users; as a preventative measure; exclusively at its expense; and for an unlimited period' [and] "which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright'.[31]

National courts have underscored this position. For example, in *GEMA v YouTube* in January 2016, the Munich court ruled that YouTube was neither directly nor indirectly liable for the uploaded content, even when it profits from videos that are infringing.[32]

Blocking injunctions must be strictly targeted

Under the net neutrality provisions adopted by the EU in 2015[33], blocking by network providers is not permitted, unless the intermediary has received a court order.

The law does permit injunctions to be ordered by the courts under a trio of provisions in the E-Commerce Directive, Copyright in the Information Society Directive, and IPR Enforcement Directive.[34] Courts across the EU have insisted that such injunctions must be strictly targeted.[35] This can been seen in cases from France, Greece, Italy, and Britain.[36] To give one example, the District Court of Athens rejected a demand by a group of collecting societies for the blocking of entire websites and granted an injunction only against specific parts of the site.[37]

There is always a risk of over-blocking. For example, the *Radio Times* was blocked following an order against a football-streaming site.[38] An intervention in the High Court by Open Rights Group has ensured that the British ISPs now publish a blocked site list for copyright blocking orders.

Hence, for a blocking order to be compatible with human rights law, in addition to the technical blocking methods, the order must state who might be affected and how long it would last, and provide a means for affected people to appeal the order.[39]

The European Court of Human Rights (ECtHR) underscored this important principle when it clarified that blanket blocking orders can never be justified. In *Yildirim v Turkey*, the concurring opinion stated that "*blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship*".[40]

The European Convention on Human Rights (ECHR) Article 10.2 provides the framework for protecting the user's freedom of expression against interference. Any restrictive measures must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate in a democratic society. Measures must be clear, precise and specific to the legitimate aim of the state. Blanket blocking of an entire site or service, for example, would not be appropriate. The consequences of a law or policy must be foreseeable and there must be a possibility for due process. The policy aims, including copyright enforcement and security, must be balanced against other competing rights, including the rights to freedom of expression, freedom of assembly and association, and privacy.

Clarity for links

Where injunctions are brought against linking sites, the issue is whether hyperlinks to copyrighted material constitute an infringement of copyright. Rightsholders have been pursuing cases in national courts against linking sites, arguing that the links do infringe. Courts across the EU have wrestled with this issue.[41]

The legal point on which these cases turn is 'communication to the public'. Under copyright law, it is a right of the author to determine where, when, and how their works are communicated to the public. If a link points to an unlicensed posting of a copyrighted work, is that link a communication and does it itself infringe? In 2014, the ECJ ruled in *Svensson v Retriever*[42] that links are an act of communication to the public under copyright law. However, where the linked content was already in the public domain, they did not require authorisation. This line of reasoning was clarified in a 2016 opinion of the Advocate General in the recent case of *GS Media v Sanoma Media*[43] that said it does not: "[H]yperlinks which are placed on a website and which link to protected works that are freely accessible on another site cannot be classified as an act of communication

within the meaning of the Copyright Directive". In other words, links to copyright-protected content do not infringe, regardless of whether the work was or was not posted with the rightsholder's authorisation. Expert opinions said that this would provide a clarity for intermediaries.[44]

The Advocate General's opinion is an especially important one because it recognised the inherent nature of linking to create the World Wide Web.[45] If users risked being sued every time they posted a link, they would stop posting, and that could have the effect of killing the entire web.

No distinction for active hosting

EU law makes no distinction between active or passive hosting. The concept of 'active hosting' has at times formed part of deliberations in the national courts and the ECJ about the role played by the intermediary. For example, in the case of *RTI v Yahoo!* there was an attempt to distinguish between active and passive providers. A Milan court considered that a passive provider would be one whose activity was limited to the technical process of operating a communications system or platform, whereas an active provider would be one who managed, catalogued, and indexed links to material uploaded by the users. This type of activity, according to the court, meant that the intermediary played an active role in the exploitation of the content. However, the appeal court ruled that no such distinction existed, and that content organisation, even for profit, was not sufficient to exclude a provider from the liability exemption.

In other words, an intermediary that catalogues or indexes content is covered by the hosting exemption in the E-Commerce Directive and they cannot be made liable for illegal content. This is a very important principle enabling intermediaries to defend their businesses, notably against copyright infringement claims.

However, the existing law does allow flexibility for courts to manoeuvre if they feel that the intermediary has intervened too much and is complicit in the infringement. In *Paramount v BSkyB*, concerning a movie-streaming site, the judgment held that the site operator had 'intervened in a highly material way'. It related to the way the site had acted to aggregate streams, categorise, reference and moderate them, and improve searchability for the purpose of quality control for registered users. However, it followed a complex reasoning, as illustrated by this extract:

"I acknowledge that it is arguable that the mere provision of a hyperlink is not enough to constitute communication to the public (particularly if the hyperlink is not directly to a source of the copyright work). I also acknowledge that it is arguable that it makes no difference whether or not the source of the copyright work to which the hyperlink links is licensed by the copyright owner. I also acknowledge that it is arguable that it makes no difference whether clicking on the links results in framing (i.e. the work being presented within the frame of the operator's website) or not. What [they] were doing, however, went beyond the mere provision of hyperlinks linking (directly) to (unlicensed) sources of copyright works (which were framed). As explained in the passage quoted above, they were intervening in a highly material way to make the copyright works available to a new audience."[46]

Stay down – incompatible with EU law

Some rightholders have demanded "notice and stay down" injunctions. "Stay down" refers to an obligation for intermediaries to ensure that once a particular file has been removed, it will never reappear on their systems. In other words, after an intermediary has received a notice that certain content is not legal, it should take this material down and ensure that the same content does not reappear.

Stay down would require intermediaries to seek out and remove repeat copies of a file for an indefinite period. Any type of stay down system would need to operate by checking newly uploaded files against a database of previously identified infringing or illegal content; a stay down system would remove, or prohibit the uploading of, any content that matched a file in the database. Stay down requires a content scanning or filtering system. Decisions would be taken on the basis of database matches and computer algorithms rather than human understanding of the law. Stay down raises concerns over the possibility for error, notably for false positives and the taking down of legal content.

Requests for stay down as a copyright enforcement measure have been rejected by national courts in France, Germany, and Italy. In 2012, the French Supreme Court, ruling in the case of *Google v Bac Films* said there is no obligation on a hosting provider to ensure that content that has been notified and removed is not re-posted.[47] The ruling quashed the notion of a stay down obligation, noting that it would impose a general obligation to monitor, and would thus be incompatible with the E-Commerce Directive. The Milan Court of Appeal, ruling on *RTI v Yahoo!*[48], followed the ECJ's rationale, saying that Yahoo! could not be liable for searching out generic content, and that a filtering or a stay down obligation would be too burdensome.

The European Court of Justice (ECJ) ruling in the *Scarlet Extended* and *Sabam v Netlog* cases (see above) supports this position. Stay down would, by its very nature, require filtering indiscriminately the content stored by all users, as a preventative measure, for an unlimited period, exclusively at the intermediary's expense. Likewise, the ECtHR ruling in *Yildirim v Turkey* provides further clarification that blanket measures applied for an indefinite time would be in violation of human rights law. Hence, any policy initiative that implies an obligation for stay down will cross the line that has been drawn by the courts, and violates the right to freedom of expression.

Self-regulatory agreements have proved controversial

Self- or co-regulatory agreements or voluntary measures are often favoured by policy makers. In the context of intermediary liability issues, however, the European Commission has not had much success with them. The Stakeholder Dialogues of 2009-2011 were an attempt by the Commission to draft a 'voluntary' scheme for copyright takedowns that ended with the internet providers walking out of the talks.[49]

There are several examples of existing self- or co-regulatory measures at the national level to address copyright enforcement, with very mixed outcomes. Britain's Digital Economy Act called for a voluntary code of conduct to be drafted and mediated by the state regulator, but this proved impossible to implement.[50] France's controversial Hadopi law was implemented, but failed in its main objective, namely disconnection of alleged infringers.[51] Only one user was disconnected, after which the scheme was disbanded. Spain has implemented a system of indirect liability targeting large copyright infringing sites, operated by an administrative enforcement body. [52] It was highly controversial when originally established under the so-called Ley Sinde and was only adopted after judicial oversight was introduced into the process.[53]

In Portugal, a strong negotiating stance by the internet service providers (ISPs) appears to have achieved a result that all parties can work with. They have a negotiated, co-regulatory agreement whereby blocking requests are analysed and transmitted via a state agency. This agency does not have the authority of a court, but the agreement does have elements of a court order. It insists on a precise and narrow targeting of the blocking request, which should list URLs, accompanied by evidence that the blocked content is infringing, as well as evidence that the rightsholders do hold the rights that they claim and that they have tried to contact the website. Rightsholders have to indemnify the network operators against costs. Even with these criteria, however, this system is not without problems, as illustrated by the case of the music blogger Josep Vinaixa, whose website was blocked despite his assertions that he was legally uploading music tracks given to him by the record labels for that purpose.[54]

Voluntary measures have also been implemented to address child sex abuse images. In the UK, the Internet Watch Foundation (IWF) maintains a block list which is circulated to network providers. Until recently, the IWF operated on the basis of content that was reported to it, but in 2015 began monitoring for content. Internationally, voluntary blocking measures for child sex abuse images are coordinated by Inhope, which operates on a very strictly limited remit. A report by the former UK public prosecutor, Lord Macdonald, says that, provided the remit is strictly limited to child sex abuse images, there is less likely to be an interference with freedom of expression or privacy rights. However, he warns against expanding the remit to adult pornographic content, or to proactive monitoring measures.[55]

The possibility for voluntary or self-regulatory measures being used to implement content restrictions was foreseen by the European Parliament in 2009, when it issued a reminder that any such measure must have safeguards for users.[56]

New Policy Proposals Imply Scaling Up of Liability

Until now, copyright has been the dominant arena for debates over content liability of intermediaries. However, the issue of terrorism has shot right to the top of the liability agenda in light of the spate of atrocities in Europe in 2015 and 2016. There is a high level of pressure for policy action to impose restrictions on online content due to a range of concerns, including terrorist propaganda, hate speech, and protection of minors. Proposals have been presented to address each of these areas.

The European Commission has announced that the E-Commerce Directive will remain intact and will not be amended – a move that has been welcomed by the intermediary industry and online free speech advocates alike. Re-opening of the E-Commerce Directive would have been highly controversial and policy makers have preferred to side-step it.

However, the Commission is proposing a series of other measures to meet policy aims related to terrorism, hate speech, and protection of minors that do involve quite drastic action against content that is not always illegal but may be "undesirable". These mea-

sures are incorporated into other legislation. The actions foreseen include blocking, filtering, suppression of links from search indexes, and dissuasive sanctions against intermediaries that do not comply. Intermediaries are additionally being encouraged to assist the authorities via their business terms and conditions. An analysis suggests that the total package will mean a scaling up of liability.

Law enforcement and the Terrorism Directive

On 16 March 2015, without any prior warning, the French cloud services and hosting company OVH learned that one of its clients' websites was subject to a government blockade. The site, *islamic-news.info*, was one of the first sites targeted under France's counter-terrorism law of 14 November 2014.[57] The law targets websites alleged to 'glorify terrorism' and puts in place a system of notice and action that has been widely criticised because it is run by an administrative authority with no judicial oversight. The websites are identified by the digital division of the *police judiciare*[58], who send notices to the website owner and hosting company. If there is no reply within 24 hours, a blocking order will be sent to the internet service providers. French journalists who specialise in terrorism commented that this particular site is 'not the most influential'. The chairman of OVH, Octave Klaba, tweeted his astonishment that this could happen to him, calling the law a 'nuclear bomb'.[59]

The French counter-terrorism law is symptomatic of what is happening around the EU, where States are becoming increasingly concerned about terrorist attacks. Law enforcement authorities are turning their attention to content that may be deemed to promote an "extremist" or jihadist agenda.[60] In Britain, the police have set up the Counter-Terrorism Internet Referral Unit (CTIRU) to address terrorist propaganda online. The CTIRU assesses the legality of content against the Terrorism Acts of 2000 and 2006, and seeks its removal from the web by notifying website operators and content hosts that the material apparently violates those companies' Terms of Service. The CTIRU is operated by the National Police Chiefs Council, which is a public authority, but there is no judicial oversight of the content removal requests, and hence no safeguards against errors. In Poland, a new law in 2016 provides for the intelligence services to suspend access to websites suspected of terrorist activity for up to four months.[61] It grants courts the power to issue blocking orders at the request of the Attorney General. Blocks must be "related to an event of a terrorist nature" and for a specified period no longer than 30 days. Urgent requests will require the approval of the Prosecutor General. However, there are concerns that the definitions are too vague and that the approval process will amount to a rubber-stamp review rather than close scrutiny.

These Member State policies are feeding into the EU, where policy is being developed under the EU Security Agenda.[62] A special unit within Europol, the EU Internet Referral Unit, was founded in July 2015 and is responsible for identifying content to be taken down or blocked and notifying intermediaries. It is based on the CTIRU model in the UK.

As a consequence, law enforcement takedown requests are escalating. When the British CTIRU was formed in 2010, it sought removal of 60 pieces of content a month. That has grown to over 4,000 per month. In total, it has requested takedown or blocking of 160,000 posts or accounts, including websites, videos, and user accounts[63], and it maintains a non-public filtering block list which is passed to internet service providers. The EU Internet Referral Unit had assessed 11,000 pieces of content and referred some 9,000 content takedowns in its first year.[64]

These volumes are still small compared with requests and takedowns related to alleged copyright infringement (which number in the millions), but the issue of terrorist propaganda has risen to the top of the political agenda. Estimates suggest that extremist content targeted for takedown will continue to grow. Just to take one example, Daesh (or Islamic State – ISIS) is said to have 70,000 Twitter accounts[65] and sends 90 tweets a minute or more than a hundred thousand tweets per day.[66]

The pressure on intermediaries will intensify under the proposed EU Terrorism Directive.[67] An amendment agreed in the European Parliament in July mandates takedown and blocking measures. It calls on Member States to take '*the necessary measures to ensure the prompt removal of illegal content publicly inciting to commit a terrorist offence […] hosted in their territory and to endeavour to obtain the removal of such content hosted outside of their territory'.*

The 'prompt removal of content' could imply several different technical actions and it is not clear which is intended. The removal of 'content hosted outside their territory' appears to be an option for states to issue a blocking action against web content where it is hosted outside EU jurisdiction. All of these measures are '*without prejudice to voluntary action*' taken by internet intermediaries, such as detecting illegal content, which implies continuous scanning and monitoring.[68]

'Necessary' is presumably a reference to Article 10.2 of the European Convention on Human Rights regarding interference with freedom of expression, as

is the requirement for all such restrictions to also be *proportionate*. The 'Twitter joke' case – where a Twitter user vented his frustration about a delayed flight by tweeting that he would blow up the airport – serves as a salient reminder that law enforcement can get it wrong. Compliance with Article 10.2 means that States must provide a robust justification for any measure and may only target speech that has been clearly defined and specified. Measures should be the least restrictive ones to meet the objective and cannot be imposed in a blanket manner. They should be subject to review over time and retracted if the need for the restriction no longer exists.

The Directive incorporates the possibility for judicial review for service providers, but there is no judicial oversight for users. It stipulates transparent procedures and adequate safeguards without specifying what these are. It says that users should be informed of the reason for the restriction, but fails to state what form that notice should take. Could this mean that a notice put up by the blocking intermediary would suffice? Would there be a public block list? When is the government compelled to notify the individual that the government has ordered the speech restriction? Council of Europe standards call for the criteria of any restriction to be made public by the State, and for a court or independent administrative authority to oversee the measures.[69]

Critically, the accompanying Recital (for guidance) recommends a possibility for legal action against internet companies that refuse to comply with orders to delete content:

"Member States should consider legal action against internet and social media companies and service providers, which deliberately refuse to comply with a legal order to delete from their internet platforms illegal content extolling terrorism after being duly notified about such specific content. Such refusal should be punishable with effective, proportionate and dissuasive sanctions."

This amendment, if adopted in the final version of the Terrorism Directive, will lead to massive uncertainty for intermediaries. It is not clear how the Directive is intended to interplay with the measures already established by Member States. Will the measures in France, Poland, and the UK be sufficient to comply? It is also not clear if the 'removal' obligation in the Directive refers to take-down of specific content or a stay-down order (though, again, such orders are inconsistent with the ECD's prohibition against monitoring obligations). The prospect of legal action and sanctions signals a policy shift from voluntary cooperative assistance to a tougher form of liability'.

Hate speech - link and content suppression

The big three social media platforms – Facebook, Twitter, and Google – face a lawsuit in France over hate speech. The UEJF, a French Jewish students group, has filed a case in the Paris courts, asking for more clarity on the way they moderate posts, tweets, and comments.[70] Facebook is also being sued in Germany over claims that it failed to remove quickly enough posts containing Nazi memorabilia.[71]

Hate speech is rising up the policy agenda as policy makers become concerned about the effects of immigration – and in Britain, the outcome of the Brexit vote.[72] The official EU definition of hate speech is "*publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin.*"[73] However, the definition of hate speech is prone to a variety of interpretations in different Member States. The European Court of Human Rights has wrestled with the issue in *Delfi v Estonia*,[74] where comments below a news article were deemed to be "manifestly unlawful" hate speech, although there is some controversy over whether the hate speech criteria were actually fulfilled.

It is therefore highly problematic to find that in the proposed revision of the Audio-visual Media Services Directive (AVMS), Article 28a, video-sharing platforms will be asked to 'protect all citizens from content containing incitement to violence or hatred'. Video-sharing platforms are any service whose purpose is the hosting of user-generated video content, or where 'a dissociable section thereof' does so. The provision is not optional, it is mandatory. If Article 28a is adopted, it threatens to alter the status of video-sharing platforms, drawing them into the regulatory framework for traditional broadcasters under the European Regulators Group for Audio-visual Media Services (ERGA).

The drafting of Article 28a is confusing and needs clarification. It seeks to introduce a system for flagging of illegal content and a ratings system, as well as age verification. It also seeks to impose an obligation on video-sharing platforms to "*define and apply*" definitions of hate speech in their terms and conditions. This would imply that they could take 'voluntary' action with the blessing of the authorities. It is encouraged by a further clause calling for a 'co-regulatory system', and for video-sharing platforms to submit codes of conduct to the ERGA. It is not clear what kind of voluntary action or co-regulatory system could be intended. The text also makes an obtuse reference to the injunctions provision in the E-Commerce Directive, suggesting that Member States

could obtain blocking orders.

The text does not explicitly call for monitoring. However, a closer interpretation of the text suggests that it would be required. Firstly, Article 28a seeks to 'protect all citizens' from hate speech. This language implies the removal of all content that could be deemed hate speech. It would mean proactive, continuous, blanket monitoring of all content. Such monitoring would not be compatible with the E-Commerce Directive. Secondly, the accompanying Explanatory Memorandum suggests that video-sharing platforms primarily 'organise' the content, therefore the obligation would "*relate to the responsibilities of the provider in the organisational sphere and do not entail liability for any illegal information stored on the platforms as such*".[75] The text implies that mere organisation would not require monitoring. However, for a video-sharing platform, the 'organisational sphere' means cataloguing, indexing, and search algorithms. 'Responsibilities' could mean actions such as keyword searches, suppressing links, or amending search algorithms.

As currently drafted, it is difficult to see how Article 28a differs from a duty of care or a stay down obligation. The compatibility of the proposed Article 28a with the E-Commerce Directive needs to be clarified. Drawing an inference from copyright case law, taking a role in organising content would not in itself bring on liability for the content, nor would linking to infringing content.

So, whilst the Directive states that it will not impose a monitoring obligation, it arguably does so by explicitly seeking changes to the platform's own terms and conditions and by suggesting manipulations to the underlying platform technology. The potential exists for over-zealous and arbitrary actions, and the risk is that it would not comply with Council of Europe standards: laws about hate speech should not be applied in a manner that would inhibit public debate about issues of democratic concern.[76]

As a separate initiative, a Code of Conduct on Illegal Hate Speech has been drawn up with the four big content platform providers – Google, Facebook, Twitter, and Microsoft – under the auspices of the EU Security Agenda. The companies have agreed to review and, if deemed appropriate, take down hate speech notified to them by authorities, NGOs, or others within 24 hours. The Code of Conduct on Illegal Hate Speech raises many concerns[77], especially because the allegedly illegal speech is to be reviewed under the individual Terms of Service of each provider – which can be more restrictive than the legal standards for "hate speech" by which the government is bound. Reviewing under the terms of service means that the criteria for making a determination are not clear, nor are the criteria for a valid policy notice. The platforms will themselves determine the take-down criteria. This is problematic given the different possible interpretations of what hate speech is. Moreover, the process calls for proactive organisation by certain privileged interest groups to feed the take-down requests to the platform providers, leading to an outsourced take-down system that will operate without any judicial oversight.

Hence, these twin proposals for hate speech, whilst they may have a well-intentioned policy aim, would seem to have the effect of leaving users exposed to arbitrary take-downs and potentially inserting an obligation to monitor through the back door.

Protection of minors - over-broad definition

Article 28a of the Audio-visual Media Services Directive contains a second proposal for video-sharing platforms regarding the protection of minors. Once again, it is broadly drafted. Minors must be protected from "*content which may impair their physical, mental or moral development*". Such language is wide open to interpretation by the intermediary and immediately raises concerns. The "*physical, mental or moral development of children*" will have different interpretations in the mind of each person reading the proposed directive. The interpretation will be influenced by the cultural, social, and ethnic background of the individual. Whilst this kind of language may have worked for an old-style broadcast environment where one-off decisions would be taken about individual programmes, it is inappropriate in in the internet context where millions of pieces of content would have to be sifted automatically. The suite of measures is the same as is proposed for hate speech – flagging, rating, age verification, and defining and applying the concepts of such content in the terms and conditions. However, in addition, video-sharing platforms could be asked to implement parental controls on their servers. This would seem to be a similar idea to the network-based parental controls implemented in the UK (see below). These parental control systems involve continuous monitoring and generally operate by means of a content filtering system. They are typically outsourced, potentially putting them outside the reach of EU law. The content-filtering software is developed by third parties[78], who define their own criteria. On the current systems implemented in the UK, categorisation is not uniform. Some systems have 8 categories, some have 17. The major suppliers of filtering systems are headquartered outside the EU, and their development methods are non-transparent. It is not known in which jurisdiction the filtering analysis is done. This raises concern if the proposed Article 28a

is to be interpreted by such systems.

Given the variability in categorisation, combined with arbitrary link suppression and lack of foreseeability, Article 28a requires clearer direction from the legislature. As currently stands, it implies a duty of care as a preventative measure for all time that would not be compatible with either the E-Commerce Directive nor human rights standards, and intermediaries will struggle to meet the requirement.

IPR enforcement – follow the trail

IPR enforcement is the subject of a policy review.[79] Measures such as notice-and-action, stay down and follow-the-money are under consideration. The European Commission previously proposed a Notice and Action directive and then shelved it, but it could be revived. Notice-and-action means more than just taking down content from a platform. It could encompass a broader range of measures, such as network-based blocking, stopping payments or advertising, and search engine de-indexing. There was controversy over the previously proposed directive because it included a counter-notice enabling website owners and users to challenge the notices.

Rightholders are demanding a 'stay down' obligation, and there have been calls for an explicit duty of care, which seems to have formed part of the European Commission's policy deliberations[80]. Such a duty of care for copyright would shift the onus onto intermediaries to take a more proactive approach. They could be asked to proactively monitor and seek out illegal content, and take it down or block it.[81] To see what a copyright duty of care could look like, there is a proposal in the French Digital Bill [Senate] from 2016 that states that online platforms should "*act with diligence and to take all reasonable, adequate and proactive measures in order to protect consumers and intellectual property right owners against the promotion, the marketing and the broadcasting of counterfeit products and contents.*"[82] A duty of care along those lines would be problematic. It implies stay down, which the French courts have already declared to be incompatible with the E-Commerce Directive[83]. The European Commission has expressed a preference for a 'follow-the-money' approach.[84] This would include, for example, asking advertising or payment services to suspend facilities. The 'follow-the-money' approach appears to be straightforward, but it risks penalising legitimate businesses. The risk is illustrated by the case of Seafile, a German company offering cloud-based file storage and synchronisation services, which was a competitor to the US-based Dropbox. Seafile went public after it was asked by PayPal to monitor customer data for illegal content and copyright infringement. According to Seafile, the basis of the request was an alleged breach of PayPal's terms of service. Seafile refused to monitor its customers, resulting in PayPal ceasing service, which meant the loss of Seafile's payment facility.[85] Following high profile media coverage, PayPal apologised and reinstated the account. A follow-the-money policy would therefore raise concerns about oversight and accountability.

The Looming Cloud of Uncertainty

These proposed new measures on responsibility for content create a cloud of uncertainty that is looming over intermediaries. The proposals addressed at achieving three important policy aims – fighting terrorism, protecting minors, and suppressing hate speech – will scale up the liability threat, and in doing so will create a significantly higher level of legal uncertainty for intermediary businesses as well as for users. Continuous monitoring, suppression of links, algorithm manipulation, and blocking orders backed up by dissuasive sanctions are onerous policy proposals that will prove difficult to comply with.

An 'obligation to monitor' by another name

The E-Commerce Directive precludes an obligation to monitor being imposed on intermediaries, and in that regard, the proposed measures outlined above raise serious questions. Any expectation that intermediaries take preventative action or should be given a duty of care will mean that the intermediary has to monitor the content on its system and take its own judgement about which content to allow or to block. Stay down measures would be especially onerous, because intermediaries would have to continuously monitor their users' activity for repeat uploads of files, which they would then take down. On that basis, any of these measures would seem to be an 'obligation to monitor' by any other name.

Compliance with such requirements has gone beyond the possibility for human decision-making. With the volume of monitoring now in the hundreds of thousands and even millions of files, the only way to comply is to install automated systems. These systems process the data using a combination of techniques such as machine learning, pattern recognition, and link analysis. The data is obtained by crawling the web and analysing user data[86]. The necessary level of investment means that only large corporations have the financial resources to do it. For example, Facebook and Vimeo[87] already use a content scanner, as does YouTube. The latter is said to have invested more than €50 million on its scanning system.[88]

The accuracy of such systems is variable. An academic study of the notice-and-takedown system in the US has indicated nearly 30% of takedown requests are of questionable validity, and frequently fail to identify videos that would be classified as fair use under US law or exceptions to copyright under EU law.

British broadband providers have invested 'seven-figure sums' in network-based parental controls and content filtering systems. These systems are intended to limit access to pornography and other content deemed harmful to children. They provide DNS blocking and URL filtering using deep packet inspection (DPI).[89] An academic study has detected over-blocking rates of 6% for network-based filtering systems.[90] Concerns of censorship are raised because their categorisation and block lists are arbitrary.[91] Business websites that have no relationship to pornography are being blocked, as well as many small websites publishing legal content, including churches[92], political campaigners, and small charities. The conference-booking page of the German organisation Chaos Computer Club was blocked in 2014.[93] Other blocking victims include The Owl and the Pussycat Centre in Scotland (a nature reserve offering children's adventure activities)[94] and Struthers London, a specialist luxury watch-making business. According to information obtained by digital rights advocates Open Rights Group, a user whose site has been blocked has little or no redress. They struggle to find anyone at the broadband providers who will listen, and the providers are passing the liability to their third-party suppliers of the filtering system. Their response is that if the third party has blocked it 'correctly,' then there is nothing that the provider can do. There is no clarity regarding what the legal basis is for 'correctly' blocking content. While Struthers London did manage to get their site unblocked, one study found that the process can take months on average. In the worst case, it took Vodafone 145 days – nearly five months – to unblock a site.[95]

The risks with self- or co-regulation

The EU favours intermediaries taking responsibility for content via some form of self- or co-regulation. This is either explicitly stated in Article 28a of the AVMS or indirectly implied, as in the Terrorism Directive.

Self- or co-regulation is an alternative route that avoids re-opening the E-Commerce Directive, which would bring with it political risk for policy makers. As we have seen with the 2009 Telecoms Package and the 2015 Open Internet Access regulations[96], corporate and civil society interests would battle over the liability provisions in Articles 12-15, and it could take years to negotiate an outcome.

However, the political risks with self- or co-regulatory initiatives are also considerable because they lead to a high level of regulatory ambiguity and legal uncertainty. Self-regulatory agreements or codes of conduct are made away from the public eye, and only rarely do citizens or policy makers have the opportunity to scrutinise them. In many cases, the terms are never made public, or are only partially made public when a court requests it.[97]

Self- or co-regulatory initiatives mean that the terms for content take-down or blocking are decided by corporate procedures instead of by public bodies or judges. If such initiatives are used to replace a court procedure, or as an alternative to one, they risk creating an environment where the providers of the networks and the content platforms take quasi-judicial decisions regarding the restriction of content that they are not equipped to do. The examples in the first section of this paper illustrate the complexities of legal judgments in this policy field. The courts often have to delve deep into the technical construction of a service before being able to determine the correct legal basis for a ruling, as shown by the extract from the *Paramount v BSkyB* ruling. Intermediaries are hardly likely to be able to go into such a level of detail. By contrast, they tend to be cautious when dealing with take-down or blocking requests, and remove content as a precautionary measure. This precautionary behaviour can lead to the erroneous takedown of legal content.

To give one example of such precautionary behaviour, eBay traders living in Isis Close and Isis Avenue in Oxfordshire found their payments were halted without explanation by PayPal, including one payment for a crochet kit. The action appears to have been due to the unfortunate co-incidence of their address and some form of keyword filtering. PayPal said that it had to scan customer accounts for terrorist references.[98] In a quite separate incident, a software engineer named Isis Anchalee found that her Facebook account was suddenly and inexplicably suspended.[99]

In another example, a Radio France Internationale reporter who specialises in covering Middle East conflicts and terrorism issues found that his Facebook account was suspended for three days because he had posted a photograph of a conflict zone showing an Islamic State flag.[100] However, some content from war zones may be important in order to inform the rest of the world what is happening. In particular, content uploaded to social media sites by citizens in conflict zones is becoming an increasingly important news source. For example, mainstream

media organisations use it to generate pictures and video clips for current affairs reports.[101]

Last year, Facebook said it had a policy of manually checking such content, and where it believed there is a genuine attempt to inform – if it can be substantiated that the material was uploaded by citizen journalists – it would leave it online.[102] Recent reports are suggesting that some social media platforms have implemented algorithmic scanning systems to seek out and take down extremist content. Little is known about the systems, but they are understood to be similar to those used for copyright.[103] If these reports are correct, it would represent a major change in content monitoring.

The concern is that if self- or co-regulatory agreements are implemented in support of a state policy, it would give discretion to the intermediary and risks leaving users, who may also be another intermediary such as an app, vulnerable to arbitrary content removals. In such a situation, users may find they have no right of appeal or redress. This would be incompatible with human rights principles. The European Convention on Human Rights, Article 10 obliges EU Member States to guarantee that citizens can receive and impart information without interference from a public authority. Article 10.2 underscores that any restriction on content should be prescribed by law and should only be carried out where it is strictly necessary to meet a legitimate aim and a pressing social need. The law should be clear and precise, and citizens should be able to foresee the consequences of their actions. Human rights principles suggest that States should oblige private actors to uphold those guarantees. The case law from the European Court of Human Rights has interpreted these principles as they apply to the internet. Blocking and filtering are regarded as interference that should be governed by Article 10.2.

Furthermore, EU law reminds Member States that if they want to implement restrictions on the internet, they must guarantee the right to due process.[104] The intention of the European Parliament was that this reminder applied as much to private actors and voluntary agreements, as to legislation.[105]

Uncertain protection for intermediaries

There is uncertainty around the legal protection of intermediaries if they institute voluntary or self-regulatory action to remove content of EU citizens. It is not clear whether they can be sued either in the case where they erroneously take down legal content, or where they fail to act against illegal content.

By contrast, in the US, intermediaries enjoy a high level of legal protection if they undertake voluntary measures. For example, the global social media platform Twitter was able to fend off a legal claim made under terrorism law by relatives of a contractor killed in Jordan. In *Fields v Twitter* it was claimed that Twitter had 'knowingly or with wilful blindness' provided "material support" to terrorist organisations by allowing ISIS to communicate via its system, and by that means, organise a terrorist attack.[106] However, the claim failed, and the ruling found in favour of Twitter[107], on the basis of a law that protects internet intermediaries. That law is Section 230 of the Communications Decency Act, which states that intermediaries cannot be treated as either the publisher or the speaker where content is posted on their systems. Additionally, Section 230 protection extends to blogs, comments, online forums, and any other entity that hosts or transmits user-generated content. Two further lawsuits have been filed on a similar basis – one by the family of a victim of the Paris attacks, and another by the family of victims of a Hamas attack.[108] US legal experts suggest that the social media companies will be able to successfully fend off such law suits using Section 230, although these two cases are yet to be heard in court.

Section 230 also provides a kind of double safety net in a 'Good Samaritan' clause. That clause means that if intermediaries take down content which they believe in good faith to be "*obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected*" they cannot be held liable by the poster of the content for their decisions to take it down. US law clearly offers protection to intermediaries against a range of damaging lawsuits[109] and protects intermediaries that take 'voluntary' action to remove content.

In the EU, there is no such affirmative protection for intermediaries. They are being targeted in the courts with claims against them for either not removing content deemed to be offensive, or for removing content in violation of freedom of expression. For example, Facebook has been hit with lawsuits in Germany concerning its alleged failure to remove hate speech. In the latest case to be filed, the allegation is that it did not remove Nazi images such as swastikas, which violate German hate speech laws. The litigants claim to have identified over 300 pages of such material. The merits of the case are yet to be heard. Facebook has responded by setting up a dedicated unit to monitor for racist posts, but it is clear that smaller intermediaries could be vulnerable if targeted by similar claims.

In France, Facebook is being pursued over an alleged violation of freedom of expression. The allega-

tion is that Facebook deactivated a user's account because he published an image that contravened its terms of service. The image was *L'Origine du Monde*[110], a painting by Gustave Courbet that hangs in the Musee d'Orsay in Paris. Anyone who looks at the painting will immediately see the issue. It is a painting of a nude woman from a very intimate perspective. It is recognized to be fine art and is considered perfectly legal in France. The user is demanding €20,000 damages, plus reinstatement of his account. The first issue to be decided was whether the French courts had jurisdiction; Facebook argued that the case should be heard in California. The case was filed in 2011, but the matter of jurisdiction was only settled in February 2016, when a Paris court decided that the French courts may hear the case.[111] The outcome of this case could provide an interesting test in light of the EU's wish to encourage policy-related self-/co-regulation based on the intermediary's terms and conditions. A positive outcome for the litigant could limit the scope for content removals.

Why this matters is because the legal uncertainty over content liability has economic consequences for the intermediaries.[112] A study by Oxera showed that if the liability rules are clearly defined and it is easy for the intermediary to comply, then businesses are more likely to be successful.[113] However, if there is too much uncertainty, it deters investment. It has a direct effect on the ability to raise finance because investors will assess the liability position as a business risk. Another study by Fifth Era conducted in five EU Member States found that regulatory ambiguity was a significant concern for over 80 percent of investors in digital start-ups. Seed funders or angel investors may shy away[114] if the effort needed to comply with the liability requirements is too high. They do not want to lose money by developing products that end up being non-compliant.[115] The more onerous the obligation, the more it risks handicapping European innovation. EU-based start-ups might go elsewhere; even small app developers might simply choose not to release their app for use in the EU.[116] Hence, legal uncertainty consolidates power with the large US-based corporations who already have market power. The unintended consequence is that European innovation would decline, and market power would become even more concentrated in an oligopoly of the global content platforms.

How Should Policy Address Intermediaries?

Responsibility for content is a problematic direction for policy. An environment where intermediaries could be sued for removing content under one set of rules and for not removing it under another, where they could be forced to install industrial strength filtering systems for suppression of content in order to meet over-broad and unclear policy aims, creates considerable legal uncertainty for internet intermediaries with real economic consequences and implications for other policy goals.

The proposed measures, whilst they seem attractive to policy makers, fail to meet the Commission's economic policy aims. Innovation could migrate to the US or other jurisdictions that have a more favourable content liability regime –the opposite goal of the Digital Single Market. To enable European industry to grow in a highly competitive global market, it needs a stable legal environment with clear rules. All measures, including those implemented under self- and co-regulation, should be compatible with the E-Commerce Directive and be compliant with ECHR Article 10.2. Best practice as presented by the Council of Europe standards[117], suggests judicial oversight and precise scoping of any measures, with a narrow and targeted aim, and well-defined obligations imposed on all of the industry interests involved.

This is especially important in the current political climate, shaped by the continuing terrorist attacks. Many policy makers see content responsibility as a convenient and pragmatic way to address an urgent political need. Security will probably continue to be the political driver for the new measures affecting intermediary liability, but EU policy makers should balance that aim against their other policy aims of building a prosperous Digital Single Market and guaranteeing an online environment that values free expression.

Acknowledgements

The author would like to acknowledge the kind assistance of the following people and organisations in preparing this paper: Francis Davey, Felix Treguer, Joanna Kulesza, Michael Rotert, EuroISPA, Application Developers Alliance, Open Rights Group, Allied for Startups.

1 http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm (Directive 2000/31/EC)
2 CDT, Speech 2.0 Free expression in the New "Digital Europe", March 2015. https://cdt.org/insight/speech-2-0-free-expression-in-the-new-digital-europe/
3 Derek E. Bambauer: Censorship V3.1, p. 13: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2144004
4 European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6 May 2015 http://europa.eu/rapid/press-release_IP-15-4919_en.htm
5 Source: Google Transparency reports. Figure cited is that for BPI and its member companies, 26 August 2016 https://www.google.com/transparencyreport/removals/copyright/?hl=en
6 Oxera, The economic impact of safe harbours on Internet intermediary start-ups, Prepared for Google February 2015, pp12-13, p14 http://www.oxera.com/getmedia/cba1e897-be95-4a04-8ac3-869570df07b1/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.aspx?ext=.pdf
7 European Court of Justice, Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV 16 February 2012 http://curia.europa.eu/juris/liste.jsf?num=C-360/10&language=EN
8 Sources: Business Insider, Some of Soundcloud's loyal users are starting to lose faith in the site; `18 November 2015. http://www.businessinsider.com/soundclouds-loyal-users-are-starting-to-lose-faith-in-the-site-2015-11
9 PRS for Music and Soundcloud reach a multi-territory licencing agreement ending legal proceedings, Press release: 21 December 2015. http://www.prsformusic.com/aboutus/press/latestpressreleases/pages/prs-for-music-soundcloud-reach-multi-territory-licensing-agreement.aspx
10 GEMA vs Spotify @DMV Press release, 13 April 2016 http://www.roba.com/2016/04/13/gema-vs-spotify-dmv/
11 Author's conversation with Michael Rotert, EuroISPA. This has been an ongoing issue, and the author has seen complaints to this effect from intemediaries since 2004.
12 Directive 2014/26/EU on collective rights management and multi-territorial licensing of musical works for online use in the internal market
13 https://gigaom.com/2014/10/02/german-publishers-accuse-google-of-blackmail-as-search-firm-axes-news-snippets/
14 Spanish Copyright Act., Article 32.2 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-11404
15 Nera Economic Consulting, *Impacto del Nuevo Artículo 32.2 de la Ley de Propiedad Intelectual Informe para la Asociación Española de Editoriales de Publicaciones Periódicas (AEEPP)*, 9 July 2015 http://www.nera.com/publications/archive/2015/impact-of-the-new-article-322-of-the-spanish-intellectual-proper.html
16 Ibid
17 For example, a London-based musician had promotional files on Megaupload – she claimed that her business was penalised when the site was taken down by the US authorities in January 2012.
18 OberLandesgericht Düsseldorf, I-20 U 59/10 of 21 December 2010; See also IPKat, Atari vs Rapidshare, Higher Regional Court of Duesseldorf Decides, published 7 January 2011. http://ipkitten.blogspot.be/2011/01/atari-vs-rapidshare-higher-regional.html
19 Bundesgerichtshof, Urteil vom 12. Juli 2012– I ZR 18/11 - Alone in the dark (Atari v Rapidshare) http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=63067&pos=6&anz=585
20 Eco, WLAN-Gesetz: Schärfere Host-Providerhaftung ist vom Tisch, press release 1 June 2016 https://www.eco.de/2016/pressemeldungen/wlan-gesetz-schaerfere-host-providerhaftung-ist-vom-tisch.html
21 Marcel Rosenbach, & Hilmar Schmundt , Funkstille auf dem Bürgersteig in Der Spiegel, 27/2013. http://www.spiegel.de/spiegel/print/d-101368303.html
22 European Court of Justice, Case C 484/14, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Advocate General Opinion, 16 March 2016. *See also* Field Fisher LLP The Free Wi-Fi Issue in Germany - How the European Court of Justice is Challenging German Liability Rules, in Lexology , 24 May 2016 http://intellectualpropertyblog.fieldfisher.com/2016/the-free-wi-fi-issue-in-germany-how-the-european-court-of-justice-is-challenging-german-liability-rules/
23 Urteil vom 12. Mai 2010 –I ZR 121/08 - Sommer unseres Lebens https://openjur.de/u/32452.html
24 eco Microresearch, Verbreitung und Nutzbarkeit von WLAN, WLAN-Zugangspunkten sowie offentlicher Hotspots in Deutschland, November 2014 https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan1.pdf
25 European Court of Justice, Case C 484/14, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Advocate General Opinion, 16 March 2016. E-commerce Directive 2000/31/EC https://www.linx.net/public-affairs/cjeu-advocate-general-argues-for-mcfadden-in-open-wi-fi-case
26 Bitkom press release: Bitkom begruesst Abschaffung der Stoererhaftung in oeffentlichen WLAN Netzen, 11 May 2016 https://www.derhandel.de/news/technik/pages/WLAN-Verbreitung-Regierung-will-Stoererhaftung-abschaffen-11832.html
27 Innocenzo Genna, Terror does not stop the Internet, radiobruxelleslibera.com, 22 March 2016; Zoya Sheftalovich Brussels Telecoms 'not back to normal', Politico 22 March 2016. https://radiobruxelleslibera.com/2016/03/22/terror-does-not-stop-the-internet/
28 Wi-Fi Calling a Must Have Service from Mobile Operators, says Strategy Analytics, press release 1 October 2015 https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2015/10/01/wi-fi-calling-a-must-have-service-from-mobile-operators-says-strategy-analytics#.V8mcGpMrJBx
29 E-commerce Directive 2000/31/EC, Articles 12 – 15.
30 Milan Court of Appeal, Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al, 7 January 2015 http://www.hlmediacomms.com/2015/02/25/the-court-of-appeal-of-milan-rules-on-yahoos-liability-with-respect-to-copyright-infringement/
31 See endnote 7.
32 OLG München, Urteil v. 28.01.2016 – 29 U 2798/15 http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2016-N-03388; http://fortune.com/2016/01/28/youtube-german-copyright-tussle/
33 Regulation (EU) 2015/2120 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R2120
34 Directive 2001/29/EC Article 8.3 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF; Directive 2004/48/EC Article 11 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF; Directive 2000/31/EC Article 12.3 and 14.3
35 "Germany, Greece, Italy and Britain' The French case is dealt with separately under 'stay down'. GmbH v Constantin Film Verleih GmbH, 24 March 2014 ; High Court of Justice, Neutral Citation Number: [2010] EWHC608(ch) 20th Century Fox v Newzbin, Judgment 29 March 2010.
36 Ibid; See also Footnote 34, 41. ECJ, C- 314/1UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, 24 March 2014 ; Milan Court of Appeal, Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al, 7 January 2015 ; High Court of Justice, Neutral Citation Number: [2010] EWHC608(ch) 20th Century Fox v Newzbin, Judgment 29 March 2010.
37 District Court of Athens, Case number 13478/2014 21 December 2014; See also Swiss Institute of Comparative Law. Blocking, Filtering And Take-Down Of Illegal Internet Content, Avis 14-067, 15 December 2015: Greece, pp 285-301 http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet
38 High Court of Justice, Premier League v BskyB , 133. Case No: HC13F02471, Neutral Citation Number: [2013] EWHC 2058 (Ch), 133. Judgment 16 July 2013 http://www.lexology.com/library/detail.aspx?g=08dcd41d-2da0-4e3d-b4d6-0d294fbd5d07
39 European Court of Human Rights, Application no 3111/10, Yildirim v Turkey, Judgment 18 March 2013. http://merlin.obs.coe.int/iris/2013/2/article1.en.html

40 Ibid
41 For an account of how this issue has been handled in the Spanish courts, see Peguera, M. Linking and secondary liability for copyright infringement. A look into the Spanish approach. https://ispliability.wordpress.com/ 18 May 2016.
42 European Court of Justice, Case no. C-466/12 Svensson v Retriever Sverige AB. See also: Graham Smith, Svensson - free to link or link at your risk? http://cyberleagle.blogspot.co.uk 5 July 2014 http://curia.europa.eu/juris/document/document.jsf?docid=147847&doclang=EN
43 ECJ, Case C 160/15 GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker, Opinion of Advocat General Wathelet 7 April 2016; http://curia.europa.eu/juris/document/document.jsf?text=&docid=175626&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=32185
44 See also: Innocenza Genna, European court rushes in rescue of hyperlinks on radiobruxelleslibera.com, 7 April 2016.
45 See also Peguera, M. Linking and secondary liability for copyright infringement. A look into the Spanish approach. On https://ispliability.wordpress.com/ 18 May 2016.
46 Arnold, J in High Court of Justice, Neutral Citation Number: [2013] EWHC 3479 (Ch). Paramount Home Entertainment v British Sky Broadcasting Ltd para 32. He is referring to a previous judgment in FAPL v Sky. My thanks to Andres Guadamuz and the Technollama blog for pointing this out.
47 Christelle Coslin and Christine Gateau [Hogan Lovells] No 'Stay Down' Obligation for Hosting Providers in France, on Society for Computers and the Law website, http://www.scl.org/site.aspx?i=ed32661
48 Milan Court of Appeal, Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al, 7 January 2015
49 http://ec.europa.eu/internal_market/copyright/licensing-europe/index_en.htm
50 See Horten, M (2013) A Copyright Masquerade, London: Zed Books. https://www.amazon.com/Copyright-Masquerade-Corporate-Lobbying-Threatens/dp/1780326408
51 Ibid
52 Ibid
53 Ibid
54 TorrentFreak, News site blocked by ISPs for embedding official YouTube videos, 29 January 2016. https://torrentfreak.com/news-site-blocked-by-isps-for-embedding-youtube-videos-160129/
55 Macdonald, K, *A Human Rights Audit of the Internet Watch Foundation*, London: Matrix Chambers, 2013 https://www.iwf.org.uk/assets/media/accountability/Human_Rights_Audit_web.pdf
56 Horten, M , 2012, The Copyright Enforcement Enigma: Internet Politics and the Telecoms Package, Basignstoke: Palgrave Macmillan. See Chapter 12. http://www.palgrave.com/br/book/9780230321717
57 Loi n° 2014-1353 du 13 Novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, Article 12 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id
58 Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC) a division of the police judiciare. See France TV Info, Cinq sites internet pronant l'apologie du terrorisme bloques par leministerede l'interieur, 16 March 2015; Olivier Tesquet, in Telerama, 16 March 2015 http://www.telerama.fr/medias/un-premier-site-bloque-pour-apologie-du-terrorisme,124094.phpl ; Hisham Aidi, France's almost funny attempt to block the web, in Al Jazeera 19 March 2015.
59 Octave Klaba's tweet: https://twitter.com/olesovhcom/status/577401572235296768
60 Jones, S, lone wolves raise the tempo of terror in Europe, in the *Financial Times*, 26 July 2016 http://www.ft.com/cms/s/0/36cc3a6c-533e-11e6-befd-2fc0c26b3c60.html#axzz4J5bOqGuL
61 Draft Act on Antiterrorist Measures of June 10, 2016 (ustawa o działaniach antyterrorystycznych, http://bit.ly/1Y25wST Source: Prof. Joanna Kuleza, University of Lodz. See also Jan Rydzak, Now Poland's government is coming after the Internet, 10 June 2016.
62 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/index_en.htm
63 Hansard, HL Deb, 4 May 2016, cW, Lord Ahmad of Wimbledon https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit#cite_note-28
64 European Commission Fact Sheet: Implementation of the European Agenda on Security: Questions & Answers, Brussels, 20 July 2016, available at http://europa.eu/rapid/press-release_MEMO-16-2594_en.htm
65 Tamara Fields v Twitter Inc., in the United States District Court Northern District Of California (Complaint, undated)
66 Counter Extremism Project http://www.counterextremism.com
67 Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015PC0625
68 EDRi & Access Now, Recommendations On Compromise Amendments To Draft Directive On Combating Terrorism, 20 June 2016 https://edri.org/files/counterterrorism/2016-EDRi-all-AMs-Terrorism-Directive.pdf
69 Council of Europe, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa
70 Bloomberg.com: Twitter, Facebook sued by French Jewish Group over Hate Speech 19 May 2016 http://www.bloomberg.com/news/articles/2016-05-19/twitter-facebook-sued-by-french-jewish-group-over-hate-speech
71 Breitbart.com German lawyers file lawsuit against Mark Zuckerberg over 'hate speech' against migrants 3 March 2016 http://www.breitbart.com/tech/2016/03/03/german-lawyers-take-mark-zuckerberg-to-court-over-hate/
72 http://www.theguardian.com/politics/2016/aug/26/politicians-rise-hate-crimes-brexit-vote-un-committee
73 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:328:0055:0058:en:PDF
74 European Court of Human Rights, Delfi v Estonia, Application no. 64569/09, Judgment, 16 June 2015 http://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]}
75 Proposal for a directive 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) 287/4, p13. See also Recital 29 and Article 28a http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0287&from=EN
76 Council of Europe, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa
77 https://cdt.org/insight/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online/
78 These third-party developers include Symantec, Nominum, Huawei, Allot Systems.
79 http://ec.europa.eu/growth/industry/intellectual-property/enforcement_en
80 European Commission, A Digital Single Market Strategy for Europe , COM(2015) 192 final, 6 May 2015 , p12 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
81 Reed Smith, A duty of care for ISPs – an own goal for the Commission? https://www.reedsmith.com/A-Duty-of-Care-for-ISPs---An-Own-Goal-for-the-Commission-06-29-2015/
82 Christine Gateau & Pauline Faron (Hogan Lovells) French "platform" regime: The saga continues after the adoption by the French Senate of the Digital Bill 10 May 2016 http://www.hlmediacomms.com/2016/05/20/french-platform-regime-the-saga-continues-after-the-adoption-by-the-french-senate-of-the-digital-bill/
83 Ibid

84 http://europa.eu/rapid/press-release_IP-14-760_en.htm
85 Stefan Beiersmann, Seafile: Paypal verlangt Bespitzelung von Kunden [UPDATE] Konto wieder eröffnet, in ZDNet.de 22 June 2016 http://www.zdnet.de/88272745/seafile-paypal-verlangt-bespitzelung-von-kunden-update-konto-wieder-eroeffnet/
86 See for example Symantec datasheet: downloaded July 2016. https://www.symantec.com/content/dam/symantec/docs/data-sheets/rulespace-en.pdf
87 Variety, Vimeo Starts Scanning Videos for Copyright Violations, 21 May 2014. http://variety.com/2014/digital/news/vimeo-starts-scanning-videos-for-copyright-violations-1201188152/
88 Urban, Karagnis & Scholfield, 2016, Notice and Takedown in Everyday Practice, SSRN-id2755628 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628
89 High Court of Justice, Cartier International v BSkyB, Neutral Citation Number: [2014] EWHC 3354 (Ch), Judgement 20 October 2014 https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqaXBscGppcGxwfGd4OjFmYTZlMzg4NDYxOGE5NzA
90 Matthew Rowe & Richard King, An Investigation into the Performance of UK Internet Providers' Web Filters, available at: http://www.research.lancs.ac.uk/portal/en/publications/an-investigation-into-the-performance-of-uk-internet-providers-web-filters(eb25c9ba-166d-4438-b513-e80db5ed768d).html
91 Matthew Rowe & Richard King, An Investigation into the Performance of UK Internet Providers' Web Filters, available at: http://www.research.lancs.ac.uk/portal/en/publications/an-investigation-into-the-performance-of-uk-internet-providers-web-filters(eb25c9ba-166d-4438-b513-e80db5ed768d).html
92 Open Rights Group Blocked project: https://www.blocked.org.uk/ See also https://www.openrightsgroup.org/blog/2011/o2-bans-church-this-christmas
93 Chaos Computer Club on the blocking of our website in UK, 5 December 2014 https://www.ccc.de/en/updates/2014/ccc-censored-in-uk
94 Alastair Tibbitt, "Big brother" web filters block access to fifty Scottish charity websites, STV 12 July 2014 http://edinburgh.stv.tv/articles/282356-anger-as-isp-web-filters-block-access-to-fifty-scottish-charity-websites/
95 Ibid Foonote 91 Matthew Rowe & Richard King, *An Investigation into the Performance of UK Internet Providers' Web Filters*, 2015 http://www.research.lancs.ac.uk/portal/en/publications/an-investigation-into-the-performance-of-uk-internet-providers-web-filters%28eb25c9ba-166d-4438-b513-e80db5ed768d%29.html
96 Regulation (EU) 2015/2120 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en
97 For example, the details of the British filtering schemes were only made public in the following court ruling: High Court of Justice, Neutral Citation Number: [2014] EWHC 3354 (Ch) Cartier International AG v British Sky Broadcasting, Judgment 17 October 2014 http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/Ch/2003/3354.html&query=Cartier&method=boolean
98 BBC Online, Thames Isis Addresses Spark Paypal Confusion 26 May 2016 http://www.bbc.com/news/uk-england-oxfordshire-36387158
99 Elle Hunt, Facebook thinks I'm a terrorist: woman named Isis has her account disabled, in The Guardian, 18 November 2015 https://www.theguardian.com/technology/2015/nov/18/facebook-thinks-im-a-terrorist-woman-named-isis-has-account-disabled
100 RSF deplores suspension of French journalist's Facebook account 23 June 2016. https://rsf.org/en/news/rsf-deplores-suspension-french-journalists-facebook-account
101 Author's conversation with Dr Colleen Murrell of Monash University, who has conducted a study of this content.
102 Source: Facebook representative speaking at Council of Europe conference on freedom of expression, 2015.
103 Joseph Mee & Dustin Voltz, Exclusive: Google, Facebook quietly move towards automatic blocking of extremist videos, Reuters 25 June 2016 http://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M; Levi Sumagaysay, Report: Facebook, YouTube automatically blocking extremist videos, in Silicon Beat, 27 June 2016 http://www.siliconbeat.com/2016/06/27/report-facebook-youtube-automatically-blocking-extremist-videos/; Counter-Extremism Project, press release, 17 June 2016 http://www.counterextremism.com/press/counter-extremism-project-unveils-technology-combat-online-extremism
104 Directive 2009/140/EC, Article 1.3a. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF
105 Horten, M The Copyright Enforcement Enigma: Internet Politics and the Telecoms Package, Palgrave Macmillan, 2012. See Chapter 12 which details the drafting of Article 1.3a
106 *Tamara Fields v Twitter Inc.*, in the United States District Court Northern District Of California (Complaint, undated)
107 Cyrus Farivar, It'll be very hard for terrorism victim's family to win lawsuit against Twitter in Ars Technica 17 June 2016 http://arstechnica.com/tech-policy/2016/06/itll-be-very-hard-for-terrorism-victims-family-to-win-lawsuit-against-twitter/
108 Gonzalez v Twitter Inc, Google Inc., & Facebook Inc. https://cases.justia.com/federal/district-courts/california/candce/4:2016cv03282/299775/1/0.pdf?ts=1466195587; Force & Fraenkel v Facebook Inc;
109 See Electronic Frontier Foundation infrographic on Section 230 https://www.eff.org/issues/cda230/infographic
110 *Le Monde, La Justice confirme que les tribunaux francais peuvent juger Facebook*, 12 February 2016 http://www.lemonde.fr/pixels/article/2016/02/12/la-justice-francaise-est-competente-pour-juger-facebook_4864381_4408996.html
111 Ibid
112 See endnote 6.
113 See endnote 6.
114 Fifth Era, The Impact of Internet Regulation on Early Stage Investment, 2014 http://static1.squarespace.com/static/5481bc79e4b01c4bf3ceed80/t/55200d9be4b0661088148c53/1428163995696/Fifth+Era+report+lr.pdf
115 Copenhagen Economics / *Edima, Online Intermediaries Impact on the EU Economy*, October 2015 http://www.europeandigitalmediaassociation.org/pdfs/EDiMA%20-%20Online%20intermediaries%20-%20EU%20Growth%20Engines.pdf
116 Zan Markan, a member of the Applications Developers Alliance.
117 Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa

ANNEXE

The dialogue with IT companies on tackling harmful content online

On 28 April 2015, the Commission adopted its European Agenda on Security for the years 2015-2020, in which it announced that it would launch an EU-level forum (the EU Internet Forum) to bring IT companies together with law enforcement authorities and civil society to help counter terrorist propaganda online, including measures addressing hate speech online and how to effectively remove harmful content. The EU Internet Forum was officially launched on 3 December 2015 – but contrary to what was promised, civil society was left out of the closed-door discussions, involving only the major IT companies and representatives of the law enforcement authorities of the EU Member States. Following the Brussels terrorist attacks on 22 March 2016, EU Ministers for Justice and Home Affairs (JHA) and representatives of EU institutions issued a joint statement to identify measures to combat terrorism at the EU level. Among the measures proposed, the signatories agreed that the Commission would "intensify work with IT companies, notably in the EU Internet Forum, to counter terrorist propaganda and to develop by June 2016 a code of conduct against hate speech online". To this end, the Commission, together with Facebook, Microsoft, Twitter, and YouTube, presented on 31 May 2016 a Code of Conduct on Countering Illegal Hate Speech Online. On 3 June 2016, CDT wrote a letter to Commissioner for Justice Věra Jourová questioning whether the practices laid down are sufficient to ensure that the rights of internet users are protected and respected. A preliminary assessment will be reported to the High Level Group on Combating Racism, Xenophobia, and All Forms of Intolerance by the end of 2016.

The fight against terrorism

The Commission presented on 2 December 2015 a Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism. The proposed Directive acknowledges the use of the internet and social media by terrorists for terrorism-related purposes, such as the dissemination of propaganda, interaction with potential recruits, and planning and coordinating operations. The Council reached a general approach on the Directive on 11 March 2016 and the European Parliament adopted its position on 4 July 2016. Both institutions have encouraged measures to remove or to block access to webpages publically inciting terrorist acts. The European Parliament has added that "(…) Member States should consider legal action against internet and social media companies and service providers, which deliberately refuse to comply with a legal order to delete from their internet platforms illegal content extolling terrorism after being duly notified about such specific content". It also introduces a new Article 14a that states that "Member States shall take the necessary measures to ensure the prompt removal of illegal content publicly inciting to commit a terrorist offence, as referred to in Article 5, hosted in their territory and to endeavour to obtain the removal of such content hosted outside of their territory. When that is not feasible Member States may take the necessary measures to block the access to such content". During the negotiation procedure in the European Parliament, there was an attempt to introduce an amendment on measures to establish the criminal liability of internet platforms, social media networks, and internet service providers. Fortunately, this provision did not make it into the final position of the European Parliament. The first trilogue negotiation took place on 14 July 2016 and they will resume in September 2016.

The Digital Single Market Strategy and the role of online platforms

On 6 May 2015, the Commission released its long-awaited Digital Single Market Strategy for Europe, its flagship policy initiative to eliminate national administrative silos and regulatory barriers in the digital economy. Part of the strategy called for a broad consultation on the role of platforms, including a broad range of online intermediaries, in the economy and society. To this end, the Commission launched on 24 September 2015 a Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, to which CDT responded in December 2015. The public consultation already hinted at a regulatory change on the liability for intermediaries, also covering "notice and action" mechanisms and the issue of action remaining effective over time (the "take down and stay down" principle).

The EU copyright framework review

On 9 December 2015, the Commission published its Communication on "Towards a modern, more European copyright framework" outlining the different issues the Commission was considering for legislative proposals to be adopted from spring 2016 onwards in areas such as limitations and exceptions, and online

platforms and enforcement of intellectual property rights (IPR). The Commission already stated that it was taking action with the involvement of different types of intermediary service providers "in setting and applying "follow-the-money" mechanisms, based on a self-regulatory approach". This process will involve rightsholders and intermediary service providers (such as advertising and payment service providers and shippers), as well as consumers and the civil society. Finally, in the Communication on copyright, the Commission also recognised that it was considering "whether any action specific to news aggregators is needed, including intervening on rights". For this purpose, the Commission presented on 23 March 2016 its public consultation on the role of publishers in the copyright value chain and on the 'panorama exception', to which CDT responded in June 2016.

Accompanying the Communication on copyright, the Commission also presented its Public consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights (IPR), to which CDT responded in April 2016. The public consultation aimed to assess whether further improvements needed to be made to the Intellectual Property Rights' Enforcement Directive (IPRED). The results of the public consultation have not yet been published.

The Audio-visual Media Services (AVMS) Directive review

On 25 May 2016, the Commission adopted a legislative proposal to amend the AVMS Directive in order to apply similar rules to linear and nonlinear audio-visual media services. In the revised text, new measures related to video-sharing platforms or on-demand services have been introduced, in particular, to protect minors against harmful content and all citizens from incitement to violence or hatred. In its Article 28a, the proposal would introduce an obligation on Member States to ensure that, within their field of responsibility, video-sharing platform providers put in place appropriate measures to: i) protect minors from harmful content, and ii) protect all citizens from incitement to violence or hatred. Proposed Article 28a does not provide a clear indication of what constitutes an appropriate measure for the purposes of the previously mentioned objectives. However, the proposed article contains a detailed list of those measures, including i) defining and applying in the terms and conditions of the video-sharing platform providers the concepts of incitement to violence or hatred, and of content which may impair the development of children; ii) establishing report and flagging of content mechanisms; iii) or providing parental control systems. In addition, the proposed article calls on Member States to encourage co-regulation for the implementation of these measures. Finally, the proposed article introduces the Union codes of conduct, which will be facilitated and developed by the Commission. Video-sharing platform providers or the organisations representing those providers will be able to submit to the Commission draft Union codes of conduct and amendments to existing ones. The proposal is currently being assessed separately by the Council and the European Parliament.

The Commission's next steps

On 25 May 2016, the Commission published its Communication on 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' setting out the Commission's conclusions and proposed actions based on its public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing, and the collaborative economy. The Commission confirmed that it would maintain the existing intermediary liability regime within the E-Commerce Directive; however, the Commission also stated its objectives for the upcoming legislative initiatives:

- The Commission would address the issues related to the proliferation on online video sharing platforms of content that is harmful to minors and of hate speech through sector-specific regulation as part of the review of the Audio-visual Media Services Directive.
- Among the different initiatives to be included in the next copyright package, the Commission will assess the role intermediaries can play in the protection of IPR and will consider amending the specific legal framework for enforcement. The Commission will also continue to engage with platforms in setting up and applying voluntary cooperation mechanisms aimed at depriving those engaging in commercial infringements of intellectual property rights, in line with a "follow-the-money" approach. To this end, the Commission will likely present the next copyright package in late September, which will include, expectedly, legislative proposals on cable and satellite, exceptions and neighbouring rights, and most likely a "duty of care".
- The Commission confirmed its plan to continue to push internet companies to 'do more' to combat various forms of illegal, harmful content online, and referred to the dialogue with IT companies towards a code of conduct on illegal hate speech online and the EU Internet Forum on terrorism

content as important examples of multi-stakeholder engagement processes aimed at finding common solutions to voluntarily detect and fight illegal or harmful material online.
• The Commission will explore the need for guidance on the liability of online platforms when putting in place voluntary, good-faith measures to fight illegal content online.
• The Commission will review the need for formal "notice and action" procedures to ensure the coherence and efficiency of the intermediary liability regime. But before considering launching any initiative, the Commission will first asses the results of the review of the AVMS Directive, the new copyright package, and voluntary initiatives such as the EU Internet Forum.