European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

Providers Liability: From the eCommerce Directive to the future

In-Depth Analysis for the IMCO Committee

EN

2017

DIRECTORATE GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

Providers Liability: From the eCommerce Directive to the future

IN-DEPTH ANALYSIS

Abstract

The study addresses the secondary liability of Internet intermediaries, namely, the issue of whether and to what extent, intermediaries —who bring together or facilitate transactions between third parties on the Internet— should be liable for, or in dependence of, illegal activities by their users. The report discusses the main issues related to the application of the Directive, and makes some suggestions for future improvements. It argues that the exemption should be maintained, since it is needed to ensure the diverse provision of intermediation services and the freedoms of the users of such services. Some updates to the current regulation may provide better guidance to Internet intermediaries, their users, and legal professionals.

IP/A/IMCO/2017-07 October 2017
PE 614.179 EN

This document was requested by the European Parliament's Committee on the Internal Market and Consumer Protection.

AUTHOR

Prof. Dr Giovanni Sartor, European University Institute of Florence.

RESPONSIBLE ADMINISTRATOR

Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT

Irene VERNACOTOLA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Policy Department A or to subscribe to its newsletter please write to:
Policy Department A: Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@ep.europa.eu

Manuscript completed in Month Year

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

CONTENTS

EXECUTIVE SUMMARY 4

1. INTERNET INTERMEDIARIES 6

The concept of an Internet intermediary 6

Some economic aspects 7

Intermediaries' secondary liability 8

The rationale for the secondary liability of Internet intermediaries 10

The problem of collateral censorship 12

2. THE LAW ON SECONDARY LIABILITY OF INTERNETINTERMEDIARIES 16

2.1 The main legal rules in the US and in the EU 16

2.2 Still the right framework? 19

How (not) to overcome liability exemptions 24

2.1.1 Who is a real host provider? 24

2.1.2 When does a host provider lose its immunity? 25

2.1.3 When does an injunction become general? 25

Passivity and immunity 26

3. A REGIME FOR THE IMMUNITIES OF INTERMEDIARIES 28

Principles for a regulation of secondary liabilities of Internet intermediaries 28

Duties of care of intermediaries 29

REFERENCES 32

EXECUTIVE SUMMARY

Background

The eCommerce Directive (2000/31/EC) provides certain categories of Internet intermediaries with a limited exemption from secondary liability, i.e., liability resulting from illegal users' behaviour. Today, in a radically changed economic and social context, there is the need to rethink the regulation by the Directive. Do we still need to protect intermediaries from secondary liability? What intermediaries should be protected and to what extent?

Aim

- Introduce the current regulation exempting Internet intermediaries from secondary liability;
- Identify the rationales of the exemption;
- Discuss the main issues concerning its application;
- Propose solutions and identify possible improvements of EU regulation on secondary liability of Internet intermediaries

Key Findings

The report first introduces the concept of Internet intermediaries, the context of their activity, and the rationales for exempting them from secondary liability:

- The Internet intermediaries—most of which are private actors— provide and maintain the infrastructures that enable the communication of information and the performance of economic and other activities over the Internet.
- They operate into economic structures that are characterised by network externalities, concentration, and multi-sided markets
- The exemption of intermediaries from secondary liability (i.e., liability for illegal activities of their users), has different possible rationales: promoting the activity of the intermediaries, preserving their business models, preventing excessive collateral censorship (i.e., preventing the intermediaries from censoring the expressions of their users). The last rationale pertains to the fact that secondary liability could induce intermediaries to excessively interfere with their users: the fear of sanction for illegal activities of the users could induce intermediaries to impede or obstruct even lawful users' activities. Excessive collateral censorship is likely to take place when there is legal or factual uncertainty and sanctions are high.

The report then considers the current rules governing the secondary liability of Internet intermediaries and addresses some critical issues pertaining to their application:

- The EU regulation of the secondary liability of Internet intermediaries was introduced in 2000, with the eCommerce Directive. It exempts intermediaries – those providing mere conduit, caching and hosting services – from secondary liability under certain conditions. In particular, host providers are only exempted as long as they do not know that they are hosting illegal content or activities. Intermediaries must terminate or prevent illegalities when ordered by competent authorities, but cannot be subject to general obligations to monitor and seek information.

- Today the leading online intermediaries have acquired huge economic power, becoming dominant players in the respective markets; they have huge financial and technological resources at their disposal and possess technologies for identifying and filtering out illegal content. It is questioned whether the exemption from secondary liability it is still needed under these new conditions.
- The scope and preconditions of the exemption from secondary liability are often challenged, in judicial and administrative decisions: (a) it is affirmed that only passive intermediaries enjoy the exemption, to the exclusion of search engines, social networks and sharing platforms; (b) it is assumed that knowledge of illegality exists also under conditions of legal uncertainty; (c) broadly scoped order to remove or prevent illegal behaviour are often enjoined.
- The report adopts a critical perspective on the latter approaches, since: (a) an active behaviour may be needed to better provide the intermediation service; (b) an intermediary may in good faith be uncertain of the legality of the communication it enables; (c) there are monitoring obligations that at the state of the art cannot be efficiently and selectively implemented.

Finally, the report provides some indications for a future regulation of the EU framework on the secondary liability of intermediaries, through an update or integration of the eCommerce directive:

- An EU regulation on the secondary liability of intermediaries is still needed, to provide harmonisation and certainty.
- The exemption from secondary liability should cover all main intermediaries, including search engines and collaborative platforms.
- The exemption should also cover "active" intermediaries as long as their engagement with the activities of their users pertains to their intermediation service; in particular, it should also cover the good faith removal of inappropriate or irrelevant materials.
- The exemption should not apply to those cases in which the users' illegal behaviour is favoured by the violation of duties of care of the intermediary.
- Duties of care the violation of which may lead to secondary liability should be specified for different kinds of enabled users' activities, distinguishing, for instance, expressive communications between users, the sending of advertisements, economic exchanges, the distribution of malicious software, etc. Business models and available means should also be considered in determining duties of care.

1. INTERNET INTERMEDIARIES

KEY FINDINGS

- The Internet intermediaries—most of which are private actors— provide and maintain the infrastructures that enable the communication of information and the performance of economic and other activities over the Internet.
- They operate into economic structures that are characterised by network externalities, concentration, and multi-sided markets
- The exemption of intermediaries from secondary liability (i.e, liability for illegal activities of their users), has different possible rationales: promoting the activity of the intermediaries, preserving their business models, preventing excessive collateral censorship (i.e., preventing the intermediaries from censoring the expressions of their users).
- The last rationale pertains to the fact that secondary liability could induce intermediaries to excessively interfere with their users: the fear of sanction for illegal activities of the users could induce intermediaries to impede or obstruct even lawful activities. Excessive collateral censorship is likely to take place when there is legal or factual uncertainty and sanctions are high.

This section introduces the concept of an Internet intermediary, presents some relevant economic aspects of their activity, discusses the rationale of exempting intermediaries from secondary liability and addresses in particular the connection between secondary liability and interference in user activity (collateral censorship).

The concept of an Internet intermediary

The Internet has contributed to disintermediation, enabling direct interactions between individuals, commercial entities and public agencies. However, intermediation has not disappeared; over the Internet new intermediaries have emerged —most of which are private actors— which play a crucial role (Yoo, 2012). They provide and maintain the infrastructures that enable the communication of information and the performance of economic and other activities over the Internet: the physical layout of cables and computers, the management of transmissions over connection lines, data storage and processing, services facilitating the creation of content and access to it, etc.

A report by the OECD (2010) proposes the following definition for Internet intermediaries: "Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."

The report distinguishes the following kinds of Internet intermediaries:

- Internet access and service providers, offering wired and wireless access to the Internet
- Data processing and web hosting providers, offering domain names, storage of web sites, and cloud services
- Internet search engines and portals, offering aid to navigation on the Internet
- E-commerce intermediaries, enabling online buying and selling
- Internet payment systems, processing online payments
- Participative networking platforms.

The recent years have seen the emergence of the so-called web 2.0: the content available on the Internet is provided by a vast and diverse range of actors, including a huge number of non-professional users. In this context, a leading role is played by content-intermediaries, enabling the creation, distribution, and access to content. They include two of the categories described above: Internet search engines and portals, and participative networking platforms. The following table distinguishes different kinds of participative platforms.

Type of Platform	**Examples**
Blogs	WordPress
Wikis, other text-based collaborations	Wikipedia
Instant messaging	WhatsApp,
Mobile	Mobile Facebook
Sites allowing feedback on written works	Amazon
Group-based aggregation	Reddit
Photo-sharing sites	Flickr
Podcasting	iTunes,
Social network sites	Facebook
Virtual worlds	Second Life
Online computer games	World of Warcraft
Video content or file-sharing sites	YouTube

Some economic aspects

Some economic aspects are relevant to secondary liability of Internet intermediaries (on the Internet economy, see Varian et al., 2004, (Yoo, 2012)).

First, some intermediation services are characterised by network externalities: larger services enjoy a competitive advantage since they enable more connections or provide more content and therefore are more attractive to users. Thus, quasi-natural monopolies emerge: a single winner tends to prevail in many sector, such as Google for searching, or Facebook for social networking. This tendency is enhanced by the fact that Internet intermediation is largely based on automated processings, so that each additional user has a very low marginal cost for the intermediary.

Secondly, the revenue model adopted by many intermediaries consists in providing content and services for free, alongside with the delivery of advertising and the collection of data, often personal. The collection of data enables platforms to improve their advertising performance (through the personalisation of ads), and to provide further services (e.g., market research) to be used internally or to be sold to third parties. New technologies for collecting, managing and analysing big masses of data provide the largest intermediaries with an additional competitive advantage relatively to smaller ones: they can enhance their strategies, and sell additional service based on their monopoly over "big data" they have collected.

Intermediaries relying on advertising operate in two-sided markets: they have different classes of clients —advertisers and users—, and take into account the interests of both. There is interdependence between advertisers and users: to satisfy advertisers the intermediary must attract users, providing the latter with a valuable service, or at least with a service that appears valuable to them. However, there is a potential conflict of interests between the two sides of the market: advertisers want the attention of users, distracting them from alternative interests and occupations (on attention markets, see Wu, 2017, and they want to target them specifically, appealing to their interests, but also to their possible weaknesses or lack of alternative information (see O'Neil, 2016); many users would prefer less distraction, more privacy, and a more accurate information on the available options. There may also be a tension between two different classes of users, i.e., providers and recipients of content. For instance, many recipients may prefer to be shielded from some content, which they find objectionable (pornography, violent or vulgar expressions, etc.) or just irrelevant to their interests. Thus, intermediaries may adopt the policy of removing or blocking such content, frustrating the communicative intent of its providers.

Free services offered without advertising, on a non-profit basis, also play an important role in the Internet ecology. An important example is Wikipedia, the most successful online encyclopaedia, which is supported by in donations, and is run by a foundation.

Finally, many intermediaries —most access providers— may offer their services via subscriptions. A limit case is WhatsApp, which sends no ads to its users, but transfers user data to its parent company (Facebook), which uses such data for advertising purposes. This behaviour led to sanctions by the EU Commission (which was misled in this regard by Facebook at the time of the merger) and by regulators in Italy and France.

Intermediaries' secondary liability

Legal systems may impose sanctions on users and intermediaries for unlawful online activities, based on different premises.

First, sanctions (civil, administrative, or criminal ones) against the users are triggered by illegal activities (defamation, fraud, threats, etc.) that the same users accomplish through the intermediary infrastructure.

Second, sanctions against intermediaries are triggered by unlawful activities initiated and accomplished by the same intermediaries (violating privacy/data protection, abusing of dominant market power, initiating illegal communications, etc.).

Third, sanctions against the intermediaries may be triggered by illegal activities initiated by their users. Here I shall only focus on this third category of sanctions,

which constitute the *secondary liabilities* of intermediaries (I use the term "secondary liability", mainly used in common law, to cover in general those liabilities which are dependent on the illegal behaviour of a third party, such as the vicarious liability of employers). In such cases, the intermediary does not initiate the wrongful activity that triggers the sanction, but rather provides the context or infrastructure that enables and facilitates the user's illegal behaviour, or magnifies its impacts. Without the platform hosting the information and enabling its transmission the wrongful communication could not take place; without the search engine, the illegal communication would not reach so many people, etc.

Legal systems can recognise the secondary liabilities of intermediaries to different extents and under different conditions. The difference may concern the conditions that are needed for secondary liability to be triggered as well as the sanctions entailed by secondary liability. Relatively to the facts originating secondary liability, we may distinguish the following possible approaches:

- Strict liability. The secondary liability of the intermediary is only dependent on the fact that the intermediation service has enabled the illegal and harmful users' behaviour: enabling the illegality is a sufficient condition for secondary liability.
- Negligence liability (broadly understood). The secondary liability of the intermediary requires further involvement by the intermediary, besides enabling the users' illegal behaviour. This further involvement may consist in knowledge that the illegal user's activity is taking place and possibly also in the awareness that such activity is or may probably be illegal. More generally it may consist in the violation of a duty of care to take measures to monitor users' behaviour, prevent harmful actions, or mitigate their effects.
- Liability under safe harbour conditions. The intermediary's liability requires a specific omission by them, such as failure to respond to removal requests. Taking the specified measure grants the exemption from liabilities.
- Immunity from sanctions. The intermediary (which meets the conditions for being exempted from liability) is immune from the sanctions that are triggered by the user's illegal activity, but is subject to orders by competent authorities, requiring the intermediaries to terminate or prevent illegal activities by their users, or to mitigate the consequences of such activities.
- Immunity from sanctions and injunctions. The intermediary is immune not only from sanctions, but also from the orders of judicial or administrative authorities. These authorities are precluded from enjoining the intermediary to interfere with the wrongful activity of its users.

Relatively to the applicable sanctions, a legal system may establish that the intermediary incurring in secondary liability is subject to the same civil, administrative or criminal sanctions that apply to the users, or to different sanctions, lower or higher than those that apply to the users, and of a different kind (e.g., administrative rather than criminal).

Given this broad set of choices for regulating secondary liability, we may wonder what kind of regime is preferable. To address this issue, we need to consider the rationale of a legal regime for intermediaries' liability, namely, what reasons may justify a choice of what of facts give rise to secondary liabilities and what sanctions are entailed by such facts.

The rationale for the secondary liability of Internet intermediaries

The Internet intermediaries under considerations play an overall positive social role (I am not considering, for instance, those intermediaries that deal will illegal exchanges in the so-called dark web). Such intermediaries enable activities that are in most cases —and considered as an aggregate— socially beneficial, and which may correspond to the exercise of fundamental rights and liberties: freedom of expression; economic freedoms; access to information, to culture and education; freedom of association and political participation, etc. So, the problem is to establish to what extent intermediaries that contribute to creating a socially beneficial communication infrastructure, should be liable for the misuse of that infrastructure by their users. For this purpose, we must consider what rationales would support on the one hand the introduction and extension of the liability exemptions and on the other hand their limitation or elimination (see Stalla-Bourdillon, 2012).

Let us first consider what reasons may justify imposing secondary liabilities upon intermediaries.

- First, there is the need to ensure that the victims of illegal online behaviour (the individuals whose reputation, privacy, IP rights, etc. have been violated) can be compensated. It is often difficult for such victims to obtain compensation from the primary infringers: the users engaging in the illegal online behaviour may be anonymous or not easily reachable; even when reachable, they may be insolvable; in any case the victims may have no easy way to determine in advance whether the offenders are reachable and solvent; the value of the case often does not justify engaging in costly proceedings. The possibility of having recourse to the intermediary, usually a business entity with financial resources, would increase the victim's chances of getting a compensation.
- Second, imposing liability on the intermediary may induce the intermediary to terminate or mitigate the consequences of the illegal behaviour of its users (e.g., remove the illegal information from a platform or block access to it, limit access by removing links and indexation, etc.)
- Third, imposing liability on the intermediary may induce the intermediary to prevent illegal behaviour of its users, adopting proactive measures that may prevent the illegal behaviour from taking place (e.g., by filtering content, excluding violators from using the platform in the future, etc.)

Note that the second and third reasons are based on the idea of "secondary regulation", namely, on the assumption that by regulating the intermediaries, public authorities induce intermediaries to regulate (to influence) the activity of their users. The direct target of the regulation are the intermediaries, but the final target are the users. This aspect of secondary liability does not necessarily entail a negative evaluation from a legal-political perspective, though it poses risks that cannot be considered here (on the dangers of techno-regulation see (Brownsword, 2008)). Since human action, and in particular communication, today takes place through an increasingly complex and flexible socio-technical infrastructure, the behaviour of the users of such infrastructure can often be most effectively regulated by directing legal norms towards the intermediaries who control that infrastructure, and can shape it in such a way that the users' behaviour is pushed in the desired direction (see Balkin 2014).

Secondary regulation of intermediaries can take different forms. Intermediaries may be requested to adopt specific actions that prevent or mitigate unlawful actions by their users (e.g., security measures, antispam filters, etc.). They may also be required to monitor the activities of their users to facilitate law enforcement (as in regulation imposing data retention). Finally, they may be subject to secondary liability for the unlawful actions of their users, to incentivise them to take whatever initiative is within their power to prevent or mitigate such actions.

Considerations pertaining to fairness would also favour secondary liability when an intermediary derives an economic profit from the activity of its users. In this case, it could be argued that since the intermediary is profiting from an activity that engenders (even though indirectly) third parties, it is fair that some of the intermediary's profits are used to cover those damages.

Finally, observe that the second and third reasons for intermediaries' liability presuppose that intermediaries have some real possibility of limiting the illegal behaviour of the latter. Should an intermediary be unable to exercise any real influence over the behaviour of its users, the punishment of the intermediary on the one hand would have no deterrent effect (it will not reduce unlawful user behaviour), and on the other hand it would be unrelated to any violation of duties of care by the intermediary.

Let us now consider the rationale for excluding or limiting the secondary liability of intermediaries. We may distinguish different reasons for not making intermediaries liable for the illegal behaviour of their users.

- First, secondary liabilities may negatively interfere with the intermediaries' capacity to maintain and develop their activity. To the extent that liabilities would force intermediaries to abandon or limit their services, they would negatively affect not only the intermediaries concerned —whose economic interests and rights would be curtailed— but also the users of the intermediaries' services. The latter would find it impossible or more difficult to engage in the activities that are enabled by such services. This would negatively interfere with the users' rights whose exercise is facilitated by the intermediaries' services (freedoms of expression, association, information, access to culture, economic initiative, etc.).
- Second, secondary liability may be incompatible with the business model of some intermediaries, a business model that may meet the preferences of their users. Providing a service for free may be incompatible with an extensive subjection to liabilities, since the income of the intermediary may not cover the cost of the resulting sanctions. This applies in particular where free service is provided on a non-profit base, without exposing users to advertising (e.g., Wikipedia).
- Third, secondary liability may induce intermediaries to excessively constrain the behaviour of their users. To avoid the risk of being punished for not having prevented, terminated, or mitigated illegal activities, the intermediaries may impede or obstruct lawful activities of their users, even activities consisting in the exercise of fundamental rights and contributing to the common good.

Some reasons for excluding or limiting secondary liability were arguably stronger in the beginning of the commercial Internet, than they are now, at least relatively to the leading commercial intermediaries. These intermediaries are highly profitable

ventures, and possess huge financial resources. They may be able to cover their secondary liabilities without having to change their business model, which is mainly based on sending targeted advertising to their users (much depends on the scope of their liabilities and on the amount of the sanctions to which they could be subject). However, the need to ensure the financial sustainability of small intermediaries, as well as of those which adopt a non-profit, no-advertising model.

The third reason is the more serious one. It is usually addressed under the heading of *collateral censorship*, a term introduced by Meyerson (1995), which is described as follows by Balkin (2014, 2309): "Collateral censorship occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech" (see also the dissenting opinion of Judges Sajo and Tsotsoria in the Delfi AS v. Estonia judgment of the European Court of Human rights (Application no. 64569/09)).

The problem of collateral censorship

Legal regulations imposing sanctions on certain communications (e.g., defamation, hate speech, prohibited pornography, IP violation) aim for a difficult balance. They are meant to deter unwanted speech but they should not deter communications that are legal and even socially valuable.

The legal quality and the social value of such a regulation should therefore be judged not only by the extent to which it successfully deters unlawful communications, but also by the extent to which it does not deter lawful communication. Ideally, it should indeed maximise the difference between its good outcome, namely the importance of the unlawful communications it deters, and its bad side effect, i.e., the importance of the set of lawful communications it deters. In other words, liabilities should not extend in such a way that the benefit of preventing additional illegal communication is outweighed by the damage of preventing additional legal communication (for an analysis of this issue in the regulation of the right to be forgotten, see Sartor, 2016)

Thus, a crucial issue in assessing the merit of extending liabilities from the performer of an unlawful action to the enabler of that actions, is whether this extension may engender over-deterrence on the enabler's side. The enabler — given its interests, capacities, and information— may react to the threat of secondary liabilities by excessively restricting the sphere of action of the performer, inhibiting lawful and socially valuable behaviour as well.

There are domains of the law where the enabler of illegal actions is made responsible for the sanctions that are triggered by these actions, at least under civil law. The typical domain is labour law, where employers are usually strictly liable for the damage that is caused by their employees (though differences exist across European legal systems, see Brueggemeier, 2004, Ch. E). Another domain is media law, where publishers are strictly liable, together with authors, to compensate pecuniary and moral damages resulting from the publication of illegal content.

What is common to these two domains is the fact that the enablers (employers or publishers) have a strong interest in the performance of the activity at issue, have the effective possibility of preventing or deterring its performance, and usually have access to the information relevant to determine its legality.

Thus, enablers have both the motivation and the capacity to intervene to restrict the performers' activity when they believe it is most probably illegal, while allowing it when it is most probably legal. Making these enablers liable for the unlawful activities of others should not induce them to excessively restrict lawful behaviour.

This constellation does not seem to apply to most Internet intermediaries, and in particular to content intermediaries, such as search engines and collaborative platforms.

These intermediaries may lack the willingness to take the risk of incurring in secondary liabilities, as well as the capacity to appreciate the extent of this risk, and the information that is needed to selectively limit it. Therefore, making them secondarily liable may lead to unwanted results.

For instance, a collaborative platform's willingness to take the risk to host a potentially illegal item depends on the platform's view of the benefit it could obtain by distributing that item, as compared the risk of adverse consequences resulting from its distribution. For commercial platforms, the advantage pertaining to the distribution of a single item lies in the marginal extent to which that item will contribute to attracting the attention of additional users to the platform, and to the advertising (or other) income that may in this way be obtained. For non-commercial intermediaries, it is determined by the importance they attribute — given their social, political, or reputational purposes— to the fact of enabling access to that content.

Since Internet intermediaries provide or facilitate access to huge repositories of information, blocking a single potentially illegal communication usually makes little difference to the achievement of their economic or other goals; on the contrary, enabling that communication may bring the risks of significant losses. Therefore, whenever an intermediary believes that there is some risk of liability, even a small one, or is anyway unable to exclude that such risk exists, it may be inclined to disable the communication.

An overly broad censorial attitude is also favoured by the fact that the intermediaries may lack the information that is needed to assess the liability risks related to a particular item. For instance, a social network may lack the information that is needed to establish whether an online posting contains false statements (which would make the post defamatory). Overly broad censorship may also be favoured by the fact that cost-effective filtering of unwanted content requires automated tools, which inevitably tend to screen out legal materials alongside illegal ones: improvements in the recall of illegalities (in the ability to classify as illegal a larger set of items that are actually so, i.e., to limit false negatives) usually leads to a deterioration in precision (the ability to classify as illegal only items that are really legal, i.e., to limit false positives).

The costs related to possible liabilities, in combination with the costs of the tools and effort that are needed to reduce liabilities, may make the activity of certain intermediaries no longer economically sustainable. Non-profit intermediaries, given their business model, are unable to sufficiently transform into income the positive externalities (the individual and social benefits to third parties) resulting from their activities, while secondary liability would force them to sustain the negative externalities (losses to third parties) that these activities generate. Consider, for instance, Wikipedia, whose articles are written by millions of unpaid contributors and are freely accessed by hundreds of millions of readers, with no distraction by advertising.

If the Wikipedia foundation — the non-profit intermediary maintaining Wikipedia— were liable to pay damages for any defamatory or otherwise illegal article distributed on the Wikipedia platform, it would have to terminate its activity.

These general considerations have different implications for different sources and conditions of liability, different kinds of sanctions, and different kinds of intermediaries.

Secondary liability works better, as a mechanism for secondary regulation, for illegalities that can be detected with ease, cost-effectiveness and precision.

This is the case, for instance, for communication to the public of copies of entire copyrighted works. The illegal nature of this activity is apparent, and software tools exist (content recognition systems) that can detect what copies of a given work occur on a platform, and recognise attempts to upload new copies. The secondary liability of the collaborative platforms that refuse to block access to copies of a specified copyrighted work would not lead to risks of overly broad collateral sanctions: the illegality is clear and cost-effective measures to terminate or prevent it are available.

Other sources of liability raise very different concerns. Consider, for instance, cases of defamation or hate speech. In such cases, it may be difficult for intermediaries to identify in advance —before receiving a notice— what messages by their users may be affected by these grounds of illegality. Even when the inquiry is focused on a specific message, consequent on a complaint, doubts may remain on whether the message is illegal, or whether, on the contrary, it is legal, and possibly even socially beneficial. The parties directly involved —on the one hand the issuer of the message and on the other hand the alleged victim of it— may have opposing views; the first may view the message as a way of expressing a legitimate opinion, advancing an individual interest or even a valuable social cause, the second may view the same message as being illegal and harmful. The intermediary concerned, in taking the decision to terminate or maintain access to the message acts like a judge between two opposite parties, a judge whose interests are to some extent involved in the case (in particular, the interest in reducing its own potential liabilities).

Liability risks may have a different impact on different kinds of intermediaries. It may be argued that big players will have less incentive to exceed in censorship than small players. In fact, the largest commercial intermediaries can effectively limit their legal risks by investing in legal reliable assessment processes and can absorb the cost of possible sanctions. Moreover, in some cases —when they consider that the communication at issue is more likely to be viewed as legal by the competent authorities— they might willingly accept the risk of the liabilities resulting from an unfavourable authoritative decision, in exchange for the possibility of obtaining a decision favourable to them. The latter decision will benefit such intermediaries not only relatively to the particular communication at issue, but also relatively to the many similar communications they are and will be enabling. Smaller intermediaries or those whose business model does not provide them with large resources, will have to take a much more cautious attitude, and acquiesce in removal requests.

The triggering conditions of secondary liability can also make a difference. Strict liability, which makes the intermediary liable based on the mere fact of having enabled an illegal activity, is more likely to induce excessive collateral censorship. Fault liabilities, especially when negligence consists in the violation of duties of care that are clearly specified and can be implemented in a cost-effective way, is less likely to induce excessive collateral censorship, since the intermediaries complying

with such duties may be sure to be on the safe side, and refrain from further censorial interventions. However, safe harbour regulation which provide immunity in exchange for an active behaviour by the intermediaries can also incentivise excessive censorship, where the requested behaviour leads to screening out potentially legal material too (as arguably is the case with the US Digital Millennium Copyright Act, see Section 6).

Finally, overly broad collateral censorship may be induced by excessive penalties. By increasing the cost of possible liabilities to the provider, high penalties provide an incentive to block or limit communications that may give rise to liabilities.

This can result in particular from (a) extending secondary liability to the compensation of unlimited moral damages, or (b) imposing of high administrative sanctions on an intermediary that fails to terminate illegal activities by its users.

2. THE LAW ON SECONDARY LIABILITY OF INTERNETINTERMEDIARIES.

KEY FINDINGS

- The EU regulation of the secondary liability of Internet intermediaries was introduced in 2000, with the eCommerce Directive. It exempts intermediaries – those providing mere conduit, caching and hosting services – from secondary liability under certain conditions. In particular, host providers are only exempted as long as they do not know that they are hosting illegal content or activities. Intermediaries must terminate or prevent illegalities when ordered by competent authorities, but cannot be subject to general obligations to monitor and seek information.
- Today the leading online intermediaries have acquired huge economic power, becoming dominant players in the respective markets; they have huge financial and technological resources at their disposal, they possess technologies for identifying and filtering out illegal content. It is questioned whether their exemption from secondary liability it is still needed.
- The scope and preconditions of the exemption from secondary liability are often challenged, in judicial and administrative decisions: (a) it is affirmed that only passive intermediaries enjoy the exemption, to the exclusion of search engines, social networks and sharing platforms; (b) it is assumed that knowledge of illegality exists also under conditions of legal uncertainty; (c) broadly scoped order to remove or prevent illegal behaviour are enjoined.
- The report critically reviews the trends just mentioned, arguing that: (a) an active behaviour may be needed to better provide the intermediation service; (b) the intermediary may in good faith be uncertain of the legality of the communication it enables; (c) there are monitoring obligations that at the state of the art cannot be efficiently and selectively implemented

This section introduces and compares the regulation of secondary intermediary liability in the US and in the EU. It then considers whether this still is a right framework in a new economic, social and technological context. It critically addresses some strategies to limit the scope of the exemption from secondary liability, focusing in particular on the connection between passivity and exemption from secondary liability.

2.1 The main legal rules in the US and in the EU

Let us now proceed to briefly recap the regulation of secondary intermediary liability in the US and in the EU. In both legal systems legislation was introduced about 20 years ago to shield intermediaries from secondary liability.

In the US, the secondary liability of Internet intermediaries was regulated by two distinct acts, having complementary scopes: the Communication Decency Act (CDA), Section 230, of 1996, addressing all violations, except federal crimes and intellectual property; the Digital Millennium Copyright Act (DMCA/OCILLA), of 1998, only addressing copyright infringements.

The CDA contains two main rules:

- Section 230 (c) (1) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
- Section 230 (c) (2) No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable

The first provision has been understood by the US judiciary as exempting Internet intermediaries (including both search engines and collaborative platforms) from any liability for the illegal behaviour of their users (for a discussion, and references, see Reidenberg et al. 2012). It is also generally assumed that intermediaries cannot be issued judicial orders to prevent or terminate illegal user activity or to remove illegal content; such orders can only be addressed to the users concerned (the content providers).

The second provision, the so-called good Samaritan rule, clarifies that the intermediaries who take the initiative to exclude or limit access to "objectionable" materials, do not lose their immunity. It is meant to override the view —affirmed in some judicial cases at the time— that the immunity requires passivity on the intermediary side. The rationale for this rule is to encourage providers to voluntarily prune objectionable materials (such as pornography, violent or offensive speech, etc.): they are not obliged to restrict access to such content, by they are not impaired (losing their immunity) if they choose to do so.

Secondary liabilities for copyright infringements are subject to a very different set of rules. According to the DMCA, an intermediary who hosts infringing content enjoys non-liability only when it:

- Has no actual knowledge that the material is infringing;
- Does not receive a financial benefit from infringing activity;
- Upon notification of alleged infringement expeditiously removes content or blocks access to it.

The key aspect of this law is the notice and take-down procedure. This procedure involves three parties: the hosting intermediary, the alleged right holder and the content provider. The intermediary preserves its immunity, if it takes down the allegedly infringing materials as soon as notified by the right-holder; however, the intermediary will make the materials available again, in case the content provider objects and the right-holder does not start legal proceedings.

The CDA and the DMCA have been subject to opposite criticisms. The CDA has been criticised for failing both to provide adequate remedies to victims of unlawful activities (defamation, violation of privacy, etc.), and to involve intermediaries in curbing online illegalities. The DMCA has been criticised for inducing censorship: to maintain their immunity, intermediaries tend to remove any allegedly illegal material as soon as they receive complaints, even frivolous ones. Removal becomes a "fait accompli' that content providers usually that do not challenge, to avoid the prospect of being involved in costly litigations (for a discussion see Lemley 2007.).

In the EU, the regulation of Internet intermediaries is based on articles 12-16 of the eCommerce Directive (2000/31/EC), and on the corresponding national

implementations (for an introduction to the Directive and to its application in the Member States, see Verbiest et al. 2007). The Directive specifically addresses three kinds of services:

- mere conduit, i.e., transmission over a communication; network of information, or access to a communication network
- caching, i.e., automatic, intermediate and temporary storage of transmitted information, to increase efficiency;
- hosting, i.e., storage of information.

It states that intermediaries are exempted from secondary liability when providing these services, under the conditions specified in articles 12-15. With regard to hosting, on which I shall focus my analysis, Article 14 specifies that host providers are exempted from liability when

a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The Directive (Article 15) specifies that intermediaries may be ordered, by competent authorities, to terminate or prevent infringements by their users, but they may not be subject to any "general obligation to monitor the information which they transmit or store" nor to "actively to seek facts or circumstances indicating illegal activity".

From this sketchy account, there emerge important differences between the US and the EU legislation. First, while the DMCA provides a special regulation for copyright infringements, the Directive does not distinguish between different violations. Second, in opposition to the broad scope of the CDA, covering any "interactive computer service", the Directive only addresses three named services: mere conduit, cashing and hosting. Third, while the CDA has been understood as excluding that intermediaries can be subject to authoritative injunctions, this is explicitly stated in the Directive. Four, while the CDA' "good Samaritan clause", explicitly includes in the liability exceptions the providers that actively engage in blocking access to "objectionable materials", recital 42 of the Directive states that the liability exemptions only cover activities having "mere technical, automatic and passive nature".

These differences point to some important issues.

First, we might wonder whether the EU should also have a separate set of rules for copyright infringements. In fact, many instances of copyright infringement can be more easily detected and assessed than other kinds of violations, and notice and action procedures for copyright violations are already in place in various EU countries.

Second, the fact that the EU Directive only addresses three kinds of service raises the issue of what regimes apply to the intermediaries that do not fall clearly into one of the protected kinds, such as search engines and participative platforms, still in their infancy in 2000.

Third, while it is undoubtedly true that subjecting intermediaries to authoritative orders is needed to protect the victims of online illegalities, important doubts remain concerning the admissibility of broadly scoped orders.

Fourth, the practice and social function of content intermediaries in today's internet ecology challenge the view that passivity is a necessary condition for immunity.

2.2 Still the right framework?

The US and EU legislations presented in Section 7 were introduced around 20 years ago, like similar regulations enacted in other countries, such as Japan and Canada. Such legislations have supported the growth the Internet economy and ecology: by reducing liability risks for intermediaries, they have facilitated the provision of intermediation services, and consequently have contributed the economic and social activities relying on those services.

However, these exemptions are now under debate, and it is questioned whether they are still appropriate. Today the leading online intermediaries no longer are small start-ups, facing strong incumbents with small resources and experimental technologies; they have acquired huge economic power, becoming dominant players in the respective markets; they have huge financial and technological resources at their disposal. For instance, Google now manages more than 90% of the web searches in Europe (*Figure 1*) while Facebook handles more that 80% of the social network usage (*Figure 2*).

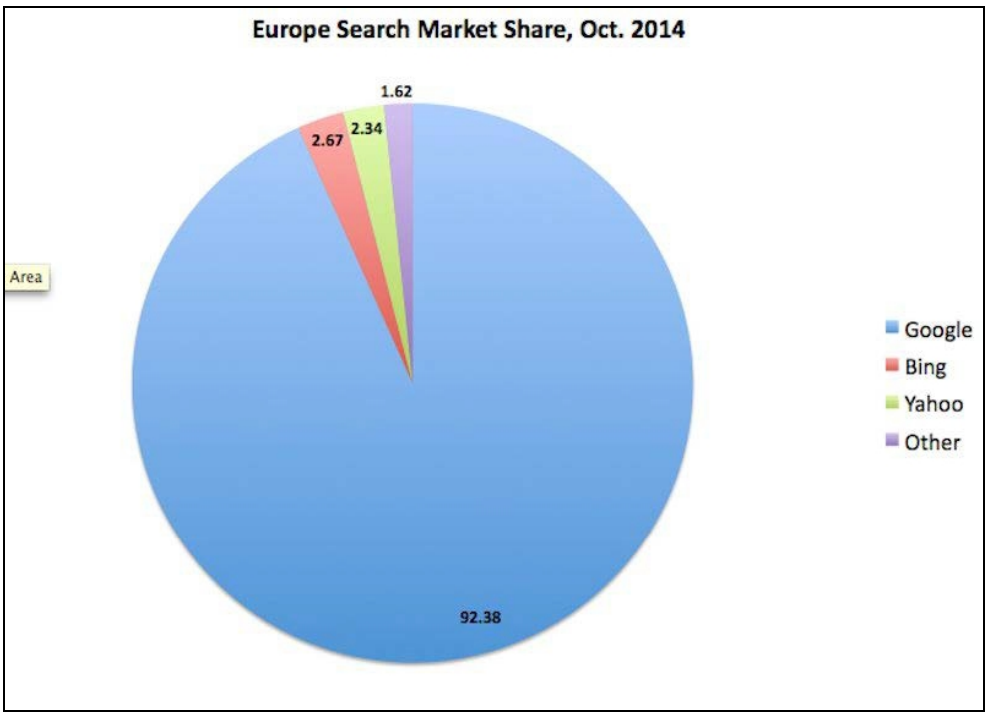

Figure 1. European Search Market Share (Source: Business Insider, 2014)

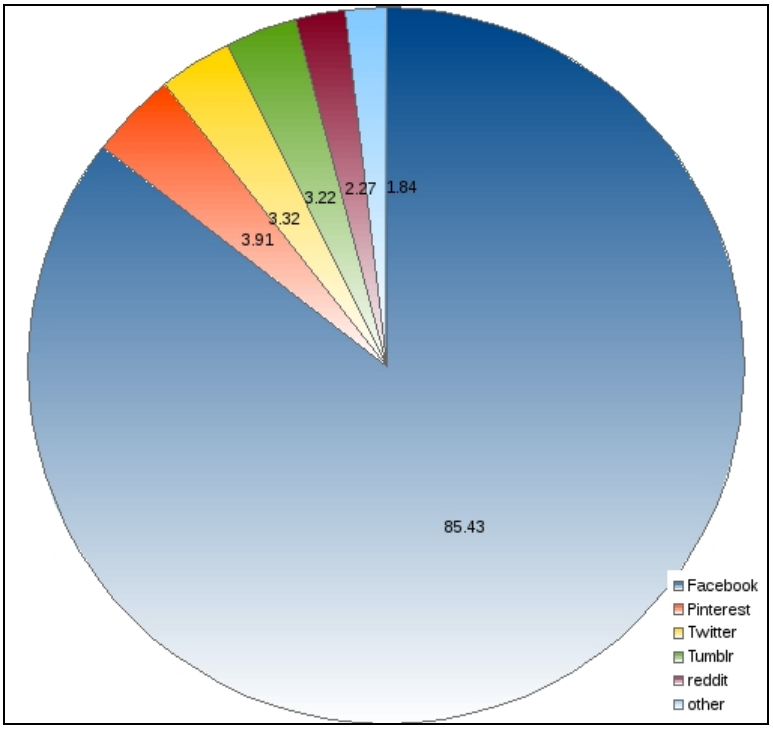

Figure 2. European Social Networks Market Share (Source: Business Insider, 2014)

This dominance, is reflected by changes in related markets, such advertising: Google and Facebook attract about one-half of the expense for online advertising (*Figure 3*), which now attracts the largest share of the total advertising expense (having overtaken television advertising, while newspaper advertising has collapsed, see *Figure 4*). The economic power of the leading intermediaries contributes to give them the capacity to influence political decisions, through lobbing or by mobilising political opinion (as happened in the US when regulations where proposed that would increase provider's liabilities and judicial powers concerning copyright infringements).

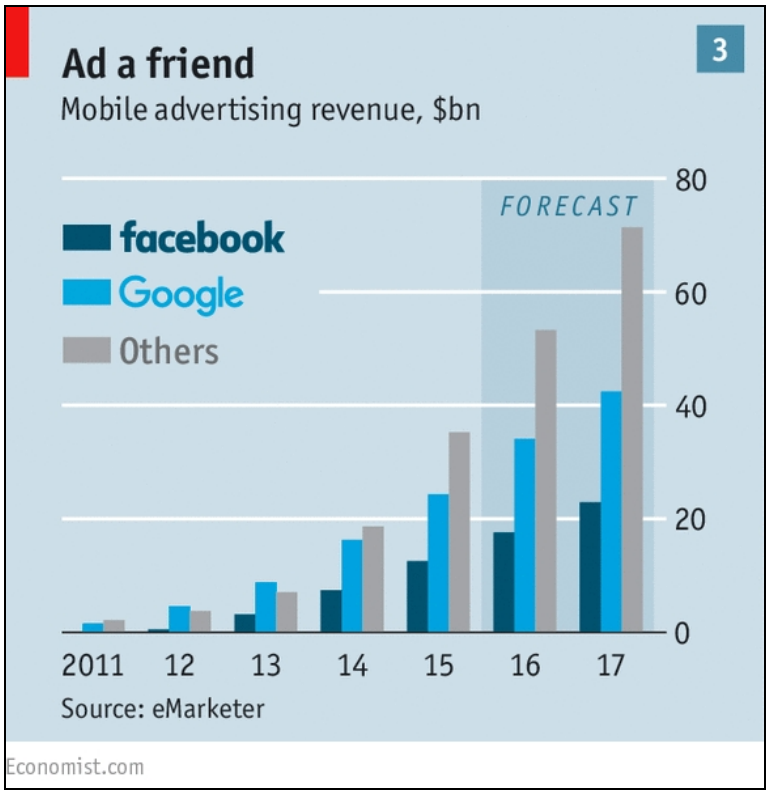

Figure 3. Mobile Advertising Market Shares

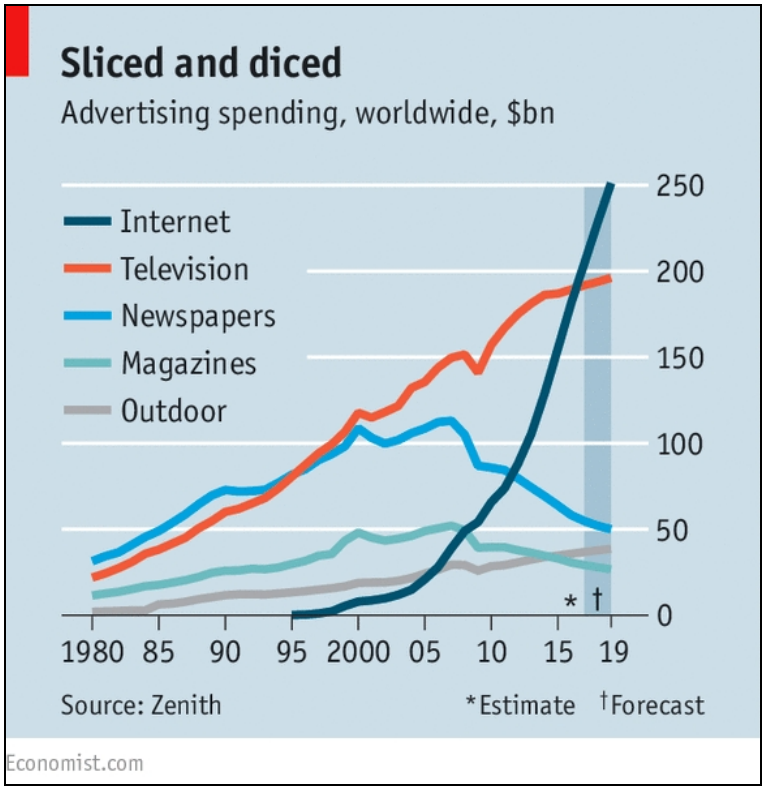

Figure 4. Advertising spending per medium

Another important development pertains to technologies for identifying and filtering out illegal content. While a human control of each piece being indexed by a search engine or made available on a platform is often unfeasible, software tools have become available that can target illegal material with increasing accuracy. Such tools are far from perfect —they risk excluding a lot of legal and socially beneficial materials, alongside with illegal ones—, but in some domains (e.g., recognition of unauthorised distribution of copyrighted works), their performance enables an effective and sufficiently precise control.

Some intermediaries are taking an increasingly active role: they contribute to frame the way in which third party content is created, they determine the way in which it is accessed, they combine further processing to that initiated by their users (e.g., indexing or linking). This is usually instrumental to the main function of the intermediary. For instance, social networks contribute to their mission —facilitating communication and social connection between their users— by providing templates through which users can prepare and organise the material they publish online; suggesting links to users having similar interests; presenting each user with the materials to which that user may be more interested, etc. Similarly, a search engine contributes to its mission —connect providers and users of online content— by indexing the content uploaded by content providers and presenting users with content that it likely to be relevant to them. As observed by Yoo (2012, Ch. 9), a certain degree of initiative, or editorial discretion, is needed for a content intermediary to effectively exercise the function to "help end users locate and obtain access to content they find desirable". Intermediaries, however, also engage in activities that are not connected to their intermediation function. For instance, they may link advertising to queries or to content, and they process user data of their own initiative. They may also frame their services in such a way that —while still meeting to a sufficient extent the preferences of their users— they are geared towards other goals, commercial or not. This may concern favouring certain communications for private purposes (which may be unfair or even illegal, e.g., prioritising certain companies in search results) or also for social purposes that are endorsed by the intermediary.

In some case intermediaries indeed play an active role that assumes political significance; they engage in controlling and manipulating certain interactions. For instance, Kent Walker, senior vice president at Google, claims that Google intervenes in the following ways to counter online extremism:

- using technology to identify (and remove) extremist videos;
- employing experts (from NGOs) to make decisions;
- putting warnings and excluding monetisation, comments and endorsement from offensive but not prohibited videos (e.g., those being both inflammatory and religious or supremacist);
- redirecting potentially radicalised users to materials that can change their mind (Walker, 2017).

As intermediaries frame and control the communications they enable, the law tends to use this capacity to regulate the activity of the users of the intermediaries' services: it establishes obligations and liabilities for intermediaries to induce the latter to prevent or restrain illegal or unwanted users' behaviour.

A most significant piece of this kind of legislation has been enacted in Germany, namely, the German Social Networks Enforcement Law (Netzwerkdurchsetzungsgesetz), adopted on 1 September 2017. Under this law, social media platforms will have to take down posts containing "obviously illegal" material within 24 hours of being notified of it. For less obviously criminal content, the compliance timeframe is seven days. If a platform repeatedly fails to meet those deadlines, it will be liable for fines of up to 50 million euros.

At the EU level, the proposed Directive on Audio-Visual Media Services (COM(2016) 287) requires Video-sharing platform providers to put in place appropriate measures to:

- protect minors from harmful content; and
- protect all citizens from incitement to violence or hatred.

The proposed Directive on Copyright (COM(2016) 593) requires host provider storing, and giving access to, large amounts of content to take adequate measures (including content recognition) to:

- implement agreements with right-holders; and
- prevent access to works identified by right-holders.

The discussion Draft of a Directive on Online Intermediary Platforms requires E-Commerce intermediaries to

- inform customers;
- remove misleading information by the supplier;
- protect consumers, on obtaining credible evidence that the supplier's conduct may unjustly harm the consumer.

Many judicial decisions require providers to actively counter illegal information or activities by their users, in order not to incur in liabilities. At the European level, we can mention the following.

- The 2014 Google-Spain decision of the European Court of Justice (Google Spain SL and Google Inc. v. Agencia Españ ola de Protecci ón de Datos (AEPD) and Mario Costeja Gonzalez, C-131/12) requires search engines to comply with a person's requests to remove unwanted links to personal information from the results of searches made on the basis of that person's name.
- The 2017 Ziggo decision by the European Court of Justice (Stichting Brein v Ziggo BV and XS4All Internet BV, C-610/15) affirmed that "a sharing platform which, by means of indexation of metadata relating to protected works and the provision of a search engine, allows users of that platform to locate those works and to share them in the context of a peer-to-peer network" engages in the communication to the public of those works (and may consequently be subject to the corresponding sanction)
- The 2015 Delfi decision by the European Court of Human Rights (Delfi AS v. Estonia, no. 64569/09)) upheld an Estonian decision punishing a journal that had failed to remove readers' online comments containing expression of hatred, in the absence of a specific complaint.

How (not) to overcome liability exemptions

At both the European and the national level, in recent years the tendency has emerged to increase pressure on intermediaries to counter illegal activities by their users. This tendency leads to various strategies meant to limit the scope of the liability exemptions provided by the eCommerce Directiv

2.1.1 Who is a real host provider?

A first strategy consists in denying that certain intermediaries are shielded by the eCommerce Directive. This conclusion is often based on the assumption that only "passive" intermediaries enjoy protection. In particular, it is argued that only "passive hosting" is covered by the concept of hosting, as used in Article 14 of the Directive. Thus, those intermediaries that store and make accessible user-generated materials, but also organise these materials, index them, link them to ads, remove unwanted items, etc., to not enjoy the protection that is granted to hosting services. This strategy is complemented by the view that toady the idea of passivity needs to be detached from the idea of automaticity: human intervention is no longer need to make a service "active", since automated processing has become flexible and selective.

As a consequence of this double move —considering that only passive intermediaries are protected, and that automated services may be non-passive— it has been denied that the social networks (e.g., Facebook), content-sharing platforms (e.g., YouTube), and search engines (e.g., Google) fall under the protection of the eCommerce Directive. This approach has been followed by the case law of various European countries.

However, arguments to the contrary can be raised too, arguing that even active intermediaries should be protected, as long as their activity pertains to their function of facilitating communications initiated by third parties.

In the following I sketch some arguments and counterarguments used to conclude that "active" intermediaries provide or do not provide a protected hosting service:

- Collaborative platforms:
  - No, they do not provide hosting, since they are not "passive", since they organise and index content, link ads to it, and remove objectionable materials.
  - Yes, they do provide hosting, since they store and make accessible content provided by third parties.
- Search engines:
  - No, they do not provide hosting, since they autonomously index web-sites and determine the outcomes of searches.
  - Yes, they do provide hosting, since they are implicitly authorised by online publishers (uploaders) to index all content on the open web, and make it accessible through an algorithm meant to satisfy user's preferences.
  -
- Newspaper hosting reader comments:

- No, they do not provide hosting, since they also provide content, and may moderate comments.
- Yes, they do provide hosting, since they enable users to upload their comments.

The idea that active host providers are not "real" host providers has gained more support in those legal systems that have implemented the eCommerce Directive in such a way as to offer host providers a stronger protection than required by the Directive. Such a protection, which may have been appropriate 20 years ago, under present conditions may appear unjust or ineffective. This is the case, for instance, with the Italian legal system. According to the Italian implementation of the eCommerce Directive (Legislative Decree n. 70 of 2003, Article 16), host providers lose their immunity when they fail to remove illegal content, "upon communication by the competent authorities"; a notice by the parties concerned is apparently insufficient to terminate the immunity. Thus, host providers are induced to remain inactive until they receive an official order, the injured parties having the burden of requesting an authoritative intervention, and in any case not being entitled to compensation (by the providers) for the damage suffered before the order is issued. To prevent this inconvenient result, the judges need to affirm the liability of host providers that fail to act on precise complaints by their users, concerning uncontroversial illegalities, even in the absence of an authoritative order. A shortcut for achieving this outcome, without explicitly contradicting the letter of the law, consists in denying that the intermediaries at issue are real "host providers" according to the law, by appealing to their active attitude.

2.1.2 When does a host provider lose its immunity?

According to Article 14 a protected host provider no longer enjoys the exemption when it remains inactive while having "actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent".

We may wonder whether the actual knowledge at issue only concerns the presence of an activity or information (which happens to be unlawful) on the platform, or whether it also includes knowledge that the information or active is unlawful.

According to the first interpretation the intermediary would lose its immunity even when there is legal uncertainty about the unlawfulness of that information; according to the second the intermediary would maintain its immunity under such circumstances. This second interpretation would correspond to the Italian text of the Directive according to which the provider loses the immunity when it is not actually aware that "l'attività o l'informazione è illecita" (the activity or information is unlawful).

The first interpretation puts more pressure on intermediaries, who may be induced not only to invest more resources in legal assessments, but also to remove any content that —given any possible legal interpretation or possible contextual facts— might be viewed as illegal by the competent authorities.

2.1.3 When does an injunction become general?

The Directive prohibits any "general obligation to monitor". This raises the issue of what activities intermediaries may legitimately be required to perform to address illegal behaviour of their users.

This issue is particularly significant in the domain of copyright infringements. Can intermediaries only be requested —by the victims, or by competent authorities— to remove single, individually identified (usually through their internet address), copies of protected works, or can they also be requested to remove all copies of a given work present in a depository (so that the provider has the burden of identifying these copies)? Can these requests extent to the preventive blocking of the reintroduction of copies of specified protected works, to the blocking of all works in a certain category (all episodes of a certain TV series), and even to all fragments of such works?

To answer these queries, the apparently descriptive concept of a "general obligation" (which delimits the sphere of the admissible orders) should become the focus of teleological interpretation. From the case law, it clearly emerges that a "general obligation" is not an obligation having a quantitatively large scope, but rather an obligation that at the state of the art cannot be efficiently and selectively implemented. The scope of this notion is also susceptible to change depending on the available technologies. For instance, removal or filtering obligations that were considered "general" when mature content identification technologies where not available (e.g., preventing all attempts to reintroduce a work in a repository), may no longer be viewed as general today, since cost-effective ways exist to identify the targeted materials. Similarly, the obligation to remove or preventively block classes of items may appear less general in those domains (such as copyright infringements or child pornography) where more cost-effective automated means to identify illegal material exist, than in domains (such as hate speech or defamation), where no such means are available (see Yannopoulos 2017).

Passivity and immunity

The regulation of secondary liability of intermediaries is meant to balance conflicting sets of goals (see Section3):

- to limit illegal online activities or mitigate their consequences, and compensate the victims of such activities;
- to preserve the viability of intermediaries' services, according to profit and non-profit business models,
- not to induce intermediaries to impede or obstruct permissible information exchanges.

To successfully implement these objectives, we must abandon the view that only "passive" intermediaries should be protected, i.e., the view that intermediaries that take a "non-passive", or "active role" —by indexing user-generated content, or linking advertising to it, or determining what results will be provided to user queries— should lose their protection from secondary liability. What justifies the exemption from secondary liability is not the passivity of intermediaries, but rather their function as communication enablers. This function would be incompatible with initiating the communications at issue, but may allow or even require playing an active role in creating an environment in which users' communications can be delivered and made accessible.

For instance, search engines provide their users with a selection of the materials available on the web, according to search algorithms that are meant to satisfy user preferences and needs, to keep users on the search engine.

This activity is entailed by the very purpose of the search engine's activity, i.e., helping content consumers retrieve material that are interesting to them, and content providers reach content-users. Therefore, it should not exclude protection from secondary liability. Similarly, the fact that a collaborative platform is active — provides tools for structuring materials, indexes such materials, connects them through links— does not entail that the platform should not enjoy protection from secondary liability.

The same conclusion holds for a newspaper hosting user-generated content. It is true that the newspaper also publishes its own content, for which it is responsible, but while hosting readers' comment the newspaper enables third party communications. The fact that the newspaper is also a content providers, should not affect its protection from secondary liability when playing the enabler's role.

Protection from intermediary liability should also not be affected by the fact that the intermediary is a business entity, operating for commercial purposes, as long as these purposes are achieved by enabling communication between third parties. The fact that advertising may be linked to user-generated content, should also not affect the exclusion from liabilities pertaining to that content. The intermediary in fact is not protected for the sake of its profit or non-profit goals, but for the way in which it enables users in achieving their communicative purposes. Therefore, the intermediary's goals should in principle be irrelevant.

In particular, the fact that intermediaries may take initiatives against illegal, inappropriate or irrelevant content or activity, should not affect their protection from secondary liability. Making the protection conditional on passivity would induce a hands-off approach that would results both in an increased quantity of online illegalities and in the failure to satisfy the users that prefer not to be exposed to objectionable or irrelevant material (these motivations explain the US good Samaritan clause). Moreover, censorship meant to satisfy the needs of the users of the intermediaries, is different from censorship motivated by the threat of legal sanctions. The first kind of censorship will only be pursued as long as it is cost-effective, and does not exclude the possibility that the censored user may switch to a different intermediary having a different audience and policy (we should, however, take into account monopolistic nature of many Internet services, which may justify a protection of users' freedom of expression against unjustified censorship by intermediaries).

Finally, note that the protection of "active" intermediaries from secondary liability is fully compatible with the subjection of these intermediaries to the liability for their own wrongful actions. Such wrongful action may pertain to the way in which the intermediary engages in the intermediation (e.g., by giving unfair precedence to its own content or products, misleading users, etc.) or in ancillary activities (e.g., processing of users' data, distributing content generated by the intermediary, etc.).

3. A REGIME FOR THE IMMUNITIES OF INTERMEDIARIES

KEY FINDINGS

- A EU regulation on the secondary liability of intermediaries is still needed, to provide harmonisation and certainty.
- The exemption from secondary liability should cover the main intermediaries, such as search engines and collaborative platforms
- It should also cover ``active'' intermediaries as long as their engagement with the activities of their users pertains to their intermediation service, including the good faith removal of inappropriate or irrelevant materials.
- The exemption should not apply to those cases in which the users' illegal behaviour is facilitated by the violation of a duty of care by the intermediary
- Duties of care the violation of which may lead to secondary liability, should be specified for different kinds of enabled users' activities, distinguishing, for instance, communications between users, the sending of advertisements, economic exchanges, the distribution of malicious software, etc. Business models and available means should also be considered in determining duties of care.

This Section will draw some conclusions concerning the principles for the regulation of secondary liabilities of Internet intermediaries, for a possible update/specification of the rules in the eCommerce directive. Then it will present some consideration of legally binding duties of care of the intermediaries.

Principles for a regulation of secondary liabilities of Internet intermediaries

The issue of regulating the liabilities of intermediaries involves two questions, the first of which is preliminary to the second:

- Do we need a special regulation limiting the secondary liability of intermediaries, or should we rather rely on the general principles of civil, administrative, and criminal law?
- Assuming that we need such a regulation, what principles should inspire it and how should they be implemented?

It may be argued that need for a special regulation for the secondary liability of intermediaries is questioned by the judicial trend toward expanding providers' liability through the "marginalization of the special Internet immunities in favour of ordinary rules" (Kohl, 2013). However, it seems to me that, the need to ensure some consistency at the European level strongly supports the need for EU regulation on the secondary liability of intermediaries. Relying on national liability principles would not only fail to provide sufficient harmonisation at the EU level, but will also fail to provide certainty at the national level, given the current confused dialectics of conflicting theories, views, and standards for decisions.

Let us now consider what could be an appropriate regime for intermediaries' liability.

First, to remain meaningful in today's Internet, a regulation of intermediaries' secondary liability should have a broad personal scope, including in particular the main content intermediaries of our times, namely, search engines, social networks and content-sharing platforms.

Second, exemptions from secondary liability should have a broad material scope, covering all kinds of illegal activities that are enabled by the intermediary. They should also cover violations of data protection law (as argued in Sartor, 2014). Some doubts in this regard were originated by Art. 1 of the eCommerce Directive, according to which this directive does not apply to question covered by the Data Protection Directive. These doubts are now resolved by Article 2 of the new General Data Protection Regulation (GDPR), according to which this regulation "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive" (see Sartor, 2013).

Third, it should be clarified that the immunity is maintained when the intermediary intervenes actively, through automated or non-automated means, to shape the service to enable third party communications, meeting the preferences of its users. This includes cases where the intermediary in good faith prevents access to objectionable material or activity (good Samaritan clause).

Fourth, the exemption from secondary liability should not exclude subjection to orders by competent authorities. The prohibition on enjoining excessively broad obligations to monitor users, to detect and prevent illegal behaviour should be maintained, possibly clarifying that the excessive broadness does not just depend on the generality of the obligation, but also on the technological possibility of implementing the obligation in a sustainable and cost-effective way, and on its impacts on users' rights.

Fifth, exemption from secondary liability should end when the provider knows or should have known of the illegitimate activity, clarifying that the knowledge that is requested includes two aspects: the knowledge that a certain piece of information or a certain activity is present on the platform, and the knowledge that this information is illegal. Under conditions of uncertainty about the legal status of a piece of information —which may depend on uncertainty about the interpretation of legal rules, but also on uncertainty about the surrounding circumstances— the exemption should be maintained.

In general, we might say that the exemptions from secondary liability should not apply when the provider contributed to the unlawful behaviour of its user by failing to exercise due care, namely, to adopt reasonable measures that could have prevented that behaviour or mitigated its effects (on duties of care of intermediaries, see Valcke et al., 2017).

Duties of care of intermediaries

The crucial issue is to determine what measures are required by reasonable due care. The assessment that the provider fails to exercise due care when it omits certain measures, should be based on several factors, such as:

- the gravity of the risk of unlawful user behaviour that the omission of the measures would entail, this risk including both the probability of such behaviour and the seriousness of the damage it may cause;
- the technologies that are available for implementing such measures;
- the economic sustainability of each measure, given the (socially beneficial) business model adopted by the intermediary;
- the way in which such measures may affect the rights and interests of the users of the intermediary.

Let us consider some examples of ways in which these criteria may operate. The availability of effective content identification technologies, and their economic sustainability, may lead to the conclusion that there is an obligation to remove or to preventively block the re-posting of the same work on the same platform. Similarly, the prohibition to provide the link to certain materials in response queries based on a person's name may extend to the future posting of copies of such materials, if such copies can be automatically identified. The availability of effective ways to control the distribution of malicious software, may lead to the liability of the intermediary that has hosted or transmitted that software (see Lichtman and Posner, 2006; van Eeten et al., 2010).

On the other hand, the request to filter out all unauthorised copyrighted works transmitted over a communication network will go beyond the required reasonable care, by excessively burdening the provider and disproportionately affecting users' rights, as argued by the EU Court of Justice in the Promusicae case (Productores de Música de España v Telefónica de España SAU, Case C-275/06,)

We should accept that in certain cases due diligence may also require preventive intervention, in particular where controls are available that enable the detection of illegal materials, minimising the risk of false positives. For example, due diligence may include the preventive screening of the reintroduction of entire copyrighted works, whose removal has already been ordered.

The legislative introduction of adequate notice and action procedures —which require an active behaviour from the intermediary who receives a notice from a person that is affected by an alleged illegality— should also be considered. As noted, the procedure prescribed by the US DMCA could lead to excessive removals, since the intermediary who removes the allegedly illegal content is protected from liability, while the uploader who fails to remove it will be liable in case the content is subsequently found to be illegal by the competent authority. A possible alternative may consist in granting immunity from sanctions to an intermediary that in good faith believes that the content is legal under circumstances of legal uncertainty, while subjecting it to removal injunctions. This may induce intermediaries to take the responsibility for adjudicating the conflict between content providers and alleged victims. Such an implied delegation of a public function to a private actor may be acceptable when both parties —the alleged right-holder and the publisher) will have easy and cheap access to remedies against an unfavourable decision by the intermediary, and when transparency is ensured.

Among the aspects to be considered in determining the extent of the intermediaries' exemption from secondary liability are the following: the extent to which the intermediary is interested in the accomplishment of each action it enables, the gravity of the damage that may be caused by illegal activities, the difficulty of identifying illegal activities, the damage that may be caused by impeding legal

activities. Based on such considerations, for instance, intermediaries should be maximally protected from liability when their intervention may affect their users' freedom of expression (whose violation also affects the right of the public to be informed), while they may be subject to a stronger obligation to take active care when they are enabling commercial transactions, including advertising, and their active intervention is needed to protect consumers, and provide security and trust.

A very important issue, on which further interdisciplinary research is needed, is the extent to which intermediaries' duties of care may be differentiated depending on the business model of the intermediary, and its economic and technological capacity.

Finally, I would like to stress the limited scope of the object of this report. On the one hand the legal obligations of intermediaries go well beyond their duties of care meant to prevent or mitigate illegal behaviour by their users; such obligations include, for instance, privacy, data protection, and consumer protection duties of providers, as well as well as their tax obligations. On the other hand, the ethical responsibilities of intermediaries may go beyond well their legal obligations (Floridi and Taddeo, 2017); such responsibilities include the need to counter anti-social activities or mitigate their effect (e.g., hate speech, fake news, etc.), and to sustain socially-beneficial practices. Both aspects are outside of the scope of this report.

REFERENCES

Balkin, J. M. (2014). Old school / new school speech regulation. *Harvard Law Review,* 2296–2342.

Brownsword, R. (2008). So what does the world need now? Reflections on regulating technologies. In R. Brownsword and K. Yeung (Eds.), *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes*, pp. 23–48. Hart.

Brueggemeier, G. (2004). *Common Principles of Tort Law*. BIICL.

Floridi, L. and M. Taddeo (2017). New civic responsibilities for online service providers. In *The responsibility of Online Service Providers*, pp. 13–42. Springer.

Kohl, U. (2013). Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (part 2). *International Journal of Law and Information Technology 21*, 187–234.

Lemley, M. A. (2007). Rationalising Internet safe harbours. *Journal on Telecommunication and High Technology Law 6*, 101–19.

Lichtman, D. and E. A. Posner (2006). Holding internet service providers accountable. *Sup. Ct. Econ. Rev. 14*, 221.

Meyerson, M. (1995). Authors, editors, and uncommon carriers: Identifying the "speaker" within the new media. *Notre Dame Law Review 71*, 79–125.

O'Neil, C. (2016). *Weapons of math destruction: how big data increases inequality and threatens democracy*. Crown Business.

OCDE (2010, April). *The Economic and Social Role of Internet Intermediaries. Report DSTI / ICCP (2009) 9 /FINAL.*

Reidenberg, J. R., J. Debelak, J. Kovnot, and T. Miao (2012). *Section 230 of the Communications Decency Act: A survey of the legal literature and reform proposals.* Technical report, Fordham Law School Center on Law and Information Policy; Fordham Law Legal Studies Research Paper No. 2046230.

Sartor, G. (2013). Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law 3*, 3–12.

Sartor, G. (2014). Case c-131/12, Google Spain and Google Inc. v. AEPD et Costeja Gonzalez. Search engines as controllers: inconvenient implications of a questionable classification. *Maastricht Journal of European and Comparative Law 21*, 564–575.

Sartor, G. (2016). The right to be forgotten: Balancing interests in the flux of time. *International Journal of Law and Information Technology 24*, 72–98.

Stalla-Bourdillon, S. (2012). Sometimes one is not enough! securing freedom of expression, encouraging private regulation, or subsidizing internet intermediaries or all three at the same time: the dilemma of internet intermediaries' liability. *Journal of International Commercial Law and Technology 7*, 154–75.

Valcke, P., A. Kuczerawy, and P.-J. Ombelet (2017). Did the romans get it right? what Delfi, Google, eBay, and UPC Telekabel Wien have in common. In L. Floridi and M. Taddeo (Eds.), *The Responsibility of Online Service Providers*, pp. 101–15. Springer.

van Eeten, M., J. M. Bauer, H. Asghari, and S. Tabatabaie (2010). The role of internet service providers in botnet mitigation. Science, Technology and Industry Working Papers 5, OECD.

Varian, H. R., J. Farrell, and C. Shapiro (2004). *The Economics of Information Technology: An Introduction*. Cambridge University Press.

Verbiest, T., G. Spindler, G. M. Riccio, and A. Van der Perre (2007). Study on the liability of Internet intermediaries. Markt/2006/09/E. Service Contract ETD/2006/Im/E2/69.

Walker, K. (2017, June 18). Four ways Google will help to tackle extremism. *Financial Times.* Wu, T. (2017). *The attention merchants: The epic scramble to get inside our heads*. Knopf. Yannopoulos, G. N. (2017). The immunity of internet intermediaries reconsidered?

Yoo, C. (2012). *The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network*. AEI Press.

CAT: QA-07-17-021-EN-C (paper)
CAT: QA-07-17-021-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT:
iStockphoto.com; Shutterstock/beboy

ISBN 978-92-846-2236-8 (paper)
ISBN 978-92-846-2237-5 (pdf)

doi:10.2861/81985 (paper)
doi:10.2861/994150 (pdf)

Publications Office

Providers Liability: From the eCommerce Directive to the future