This deliverable carries out a summary of the fundamental legal research conducted in the EXPERIMEDIA project by the legal partner ICRI-KU Leuven. It also contains a list of policy recommendations that were articulated on the basis of the conducted legal research as well as the lessons learned when assisting the EXPERIMEDIA experiments in achieving legal compliance.
<table>
<thead>
<tr>
<th>Project acronym</th>
<th>EXPERIMEDIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full title</td>
<td>Experiments in live social and networked media experiences</td>
</tr>
<tr>
<td>Grant agreement number</td>
<td>287966</td>
</tr>
<tr>
<td>Funding scheme</td>
<td>Large-scale Integrating Project (IP)</td>
</tr>
<tr>
<td>Work programme topic</td>
<td>Objective ICT-2011.1.6 Future Internet Research and Experimentation (FIRE)</td>
</tr>
<tr>
<td>Project start date</td>
<td>2011-10-01</td>
</tr>
<tr>
<td>Project duration</td>
<td>36 months</td>
</tr>
<tr>
<td>Activity 5</td>
<td>Legal, sustainability and promotion</td>
</tr>
<tr>
<td>Workpackage 5.1</td>
<td>Legal, ethical and regulatory framework</td>
</tr>
<tr>
<td>Deliverable lead organisation</td>
<td>KU Leuven</td>
</tr>
<tr>
<td>Authors</td>
<td>Pieter-Jan Ombelet (KU Leuven)</td>
</tr>
<tr>
<td></td>
<td>Aleksandra Kuczcerawy (KU Leuven)</td>
</tr>
<tr>
<td></td>
<td>Peggy Valeke (KU Leuven)</td>
</tr>
<tr>
<td>Reviewers</td>
<td>Stephen C Phillips (IT Innovation)</td>
</tr>
<tr>
<td></td>
<td>Sandra Murg (JRS)</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Dissemination level</td>
<td>PU</td>
</tr>
<tr>
<td>Due date</td>
<td>PM36 (2014-09-30)</td>
</tr>
<tr>
<td>Delivery date</td>
<td>2014-09-30</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Executive Summary ........................................................................................................... 4  
2. Introduction ......................................................................................................................... 5  
3. Summary of the Fundamental Research ............................................................................. 6  
   3.1. Privacy and Intermediary Liability .............................................................................. 6  
      3.1.1. Internet Intermediaries and Freedom of Expression ........................................... 6  
      3.1.2. Situation of Search Engines .............................................................................. 8  
   3.2. Media Law ..................................................................................................................... 12  
      3.2.1. What if Television Becomes Just an App? ......................................................... 12  
      3.2.2. Who’s Author, Editor and Publisher in User-Generated Content? ...................... 14  
   3.3. Conclusion .................................................................................................................... 15  
4. Policy Recommendations ................................................................................................... 17  
   4.1. Privacy and data protection ....................................................................................... 17  
      4.1.1. Responsibility for Processing Personal Data in Research Projects ..................... 17  
      4.1.2. Legal Ground for Processing Personal Data in Research Projects ..................... 17  
      4.1.3. Transparency ........................................................................................................ 18  
   4.2. Intermediary Liability .................................................................................................... 18  
      4.2.1. Situation of Search Engines .............................................................................. 18  
      4.2.2. Safeguards for Freedom of Expression in the Notice-and-Take Down mechanism .................................................................................................................. 19  
   4.3. Media Law .................................................................................................................... 20  
5. Conclusion .......................................................................................................................... 21
1. Executive Summary

Deliverable D5.1.7 aims to summarize the legal research conducted in EXPERIMEDIA. The legal partner KU Leuven conducted research in three main focus areas crucial for EXPERIMEDIA: privacy and data protection, intermediary liability and media law. The conducted research was presented and discussed with an international scientific community in the form of papers, conference presentations and workshops. A summary of the main findings is presented in Section 3 of this deliverable. Furthermore, the goal of deliverable D5.1.7 is to provide policy recommendations (Section 4 of the deliverable). The presented recommendations are based on the research findings, as well as problems encountered when assisting project partners in achieving compliance with the applicable laws. These recommendations are generally directed to the policy makers but in some cases, when indicated in the text, they are directed to the researchers participating in the EU research frameworks and to experimenters conducting research in the area of Future Media Internet.
2. Introduction

In this deliverable we present a summary of the fundamental legal research done in EXPERIMEDIA. The deliverable describes scientific research conducted by the legal partner ICRI – KU Leuven in the three areas relevant for the project: privacy, intermediary liability and media law. Results of the research were initially presented in the following scientific publications:

- Working paper on ‘Search engines after Google Spain: internet@liberty or privacy@peril? Brendan Van Alsenoy, Aleksandra Kuczerawy and Jef Ausloos’;
- Research report on ‘NoC Report on Internet Intermediaries Liability – Case Study: European Union & Google Spain’, Aleksandra Kuczerawy and Jef Ausloos;
- Journal article on ‘Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative’, Aleksandra Kuczerawy;
- Working paper on ‘What if Television Becomes Just an App? Re-Conceptualising the Legal Notion of Audiovisual Media Service in the Light of Media Convergence’, Peggy Valcke and Jef Ausloos and
- Book chapter on ‘Who’s Author, Editor and Publisher in User-Generated Content?’, Peggy Valcke, Marieke Lenaerts and Aleksandra Kuczerawy.

Part two of the presented deliverable provides a list of policy recommendations. They are focused on the same legal research areas that were in the centre of this project. The articulated policy recommendations address issues that were examined during the project. The provided recommendations are directed to the policy makers but also to fellow researchers who might encounter similar obstacles in their projects. The purpose of this activity is to indicate problems and their possible solutions as one of the outcomes of the project.

1 Brendan Van Alsenoy, Aleksandra Kuczerawy and Jef Ausloos, “Search engines after Google Spain: internet@liberty or privacy@peril?”, ICRI Research Paper 15, 6 September 2013, 74 p.
3. Summary of the Fundamental Research

3.1. Privacy and Intermediary Liability

In recent years, the amount of personal data available on the Internet has exponentially grown to astronomical proportions. As this data is easily retrievable through the use of search engines, people are increasingly worried about the information concerning them that can be found online. Will a potential employer see embarrassing pictures of my past? Will it emphasise my ‘misdeeds’ over my ‘good’ behaviour? These and other questions reflect some of the privacy concerns that data subjects are encountering when they come across data regarding their life on the Internet. Intermediaries, such as search engines or hosting service providers, play an important role in this process. This is because they facilitate access to information that previously could have stayed hidden in the past. Considering that some of this information might interfere with one’s privacy, a call for a balanced approach seems reasonable. Moreover, such great power to influence people’s lives should be followed by (at least) some responsibility. The role of intermediaries in providing access to information is therefore a great research topic. The objective the authors put forth was to analyse the interaction between three branches of law: privacy and data protection, intermediary liability and freedom of expression.

ICRI – KU Leuven examined these questions extensively in three academic publications. The first one focused on the EU regulation of the intermediary liability, the E-Commerce Directive, which is currently under the review process. Two other publications focused on the recent landmark case of the Court of Justice of the European Union on Google Spain. This case is a textbook example of where these three legal domains overlap. Specifically, the authors analysed if intermediaries can be held liable for the interferences in one’s right to personal image, identity and freedom. These three publications and their main findings are summarized in the following section of the deliverable.

3.1.1. Internet Intermediaries and Freedom of Expression

In the European Union, the liability of Internet intermediaries is regulated by Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive, ECD). In its section 4, the ECD contains provisions on liability exemptions for three types of services of intermediaries, namely mere conduit (article 12), caching (article 13) and hosting (article 14). These service providers can be exempt from liability when their activity is “of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.”

In these cases, the Directive provides for a horizontal exemption regime. It covers various types of illegal content and activities (infringements on copyright, defamation, content harmful to

---

9 Recital 42 of the E-Commerce Directive
minors, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect).10

Due to their role as facilitators in accessing content, Internet intermediaries are often seen as natural candidates to keep the internet ‘clean’.11 It is in their power to either remove infringing online content or help identifying wrongdoers. This may lead, however, to a situation where public policy is enforced by private entities.

The main argument to engage intermediaries in eliminating illegal online content is provided in Article 14 of the E-Commerce Directive. This provision includes conditions for liability exemptions for hosting service providers. To remain immune, providers of these services must react to notifications of illegal content. This is called a ‘Notice-and-Take Down’ procedure. However, this article has received a lot of criticism as it creates an “incentive to systematically take down material, without hearing from the party whose material is removed”.12 This does not coincide with the freedom of expression. Chilling effects on the freedom of expression will arise when hosting service providers systematically choose the cautionary approach and act swiftly upon any indication of illegality, without engaging in any balancing of rights.

Moreover, the burden imposed on these hosting service providers cannot be underestimated. Imposing an obligation on these providers to assess the legitimacy of every complaint from a third party has been called unfair.13

Lastly, criticism has risen regarding the principle of proportionality and due process.14 The E-Commerce Directive does not provide any safeguards regarding the balancing of fundamental rights, and leaves this subject matter entirely to the discretion of the Member States. The Directive encourages self-regulation (Article 16 and Recital 40), but only few Member States have introduced these self-regulatory measures. For instance, most Member States have yet to introduce a basic requirement for hosting providers to inform content providers of any complaints regarding their content.15

Cognisant of these problems, the EU has decided to review its rules on the Intermediary liability. The process started with a public consultation in 2010.16 The consultation revealed that the majority of respondents did not see a need for a revision of the Directive as a whole. Some of

---

them, however, expressed their concern about the limited protection for freedom of expression offered by the Directive. Many respondents indicated the need to clarify the issue of intermediaries’ liability for third-party content. The ‘notice-and-take down’ procedures were considered to be the most problematic aspect.\(^\text{17}\) The European Commission concluded that procedures aimed at eliminating illegal online content should be further improved. Mainly, they should lead to a quicker takedown, but at the same time should better respect fundamental rights and should increase legal certainty for online intermediaries.\(^\text{18}\) Based on these findings the Commission decided to focus its efforts on developing a new European framework for Notice-and-Action.\(^\text{19}\) In the accompanying documents the EC provided an extensive explanation of the most problematic issues that should be tackled through the initiative. The most relevant ones, from the perspective of freedom of expression, were presented in the KU Leuven publication. The examined topics included legal uncertainty and fragmentation as well as specific Notice and Take down issues such as abusive notices, counter-notifications, or the required response time. Furthermore, responses to the 2012 consultation were analysed.\(^\text{20}\)

### 3.1.2. Situation of Search Engines

#### 3.1.2.1. Liability of Search Engine Providers

The Google Spain case relates to services provided by search engines. Here as well, the three branches of law interact. Location tool services, or search engines, are covered by the definition of the Information Society Service from the E-Commerce Directive but do not fall under any of the three services described under Section 4 (cf. supra). Search engines are only mentioned in the Final Provisions of the Directive as a topic that should be analyzed further when re-examining the document.\(^\text{21}\) Therefore, as the Directive doesn’t address liability issues of search engines, the approaches in the different Member States are widely varied, ranging from considering their services to be hosting services (Hungary\(^\text{22}\), Portugal\(^\text{23}\) and Spain\(^\text{24}\)) to merely applying the general rules of law (United Kingdom\(^\text{25}\)).

---


20 Directive 2000/31/EC, art. 21(2): “In examining the need for an adaptation of this Directive, the report shall in particular analyze the need for proposals concerning the liability of providers of hyperlinks and location tool services…”


The different national approaches undoubtedly create a situation of legal uncertainty that is problematic for the providers of these search engine services. For instance, this uncertainty has led to a variety of decisions in the different European courts on Google’s legal situation.26

Another concern is that, if the legal situation of search engines is not harmonized in the European Union, an increasing amount of major multinational selection intermediaries might choose to comply with the US law, which provides them with the necessary liability exemptions to ensure their lawful operation.27

3.1.2.2. Search Engines and Data Protection Law

In the paper entitled ‘Search engines after Google Spain: internet@liberty or privacy@peril?’, the authors analyzed the questions that were asked to the CJEU in the case Google Spain. After an extensive analysis of the different rights and issues at stake, they concluded, prior to the Court’s final judgment, that search engine providers fall within the remit of European data protection law. As ‘controllers’, they process personal data in the meaning of Directive 95/46. Article 2(b) defines the ‘processing of personal data’ as

> ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.’

Moreover, if the processing takes place via an establishment located in the EU, from where they for instance sell targeted advertising space, they also fall within the territorial scope of the Directive. This conclusion is in line with the Article 29 Working Party’s opinion on search engines.28 In this opinion, the Working Party stated that a Member State should apply its national law if an establishment of the provider that is based in their territory, plays a relevant

---


26 Court of Appeal, Case no. 08/13423, 26 January 2011 (Socie´te´ des Auteurs des Arts visuels et de l’Image fixe (SAIF) v Google France/Google inc.); The Court of Appeal of Brussels, Case no. 2007/AR/1730, 5 May 2011 (Copiepresse v. Google); Court of Milan, Case no. 1972/2010, 24 February 2010.


role in the processing at issue.\textsuperscript{29} This was the second important conclusion of the paper, and was later confirmed by the CJEU in the Google Spain Grand Chamber judgment.\textsuperscript{30}

As these providers of search engine services fall within the remit of Directive 95/46, they have to comply with the data controllers’ obligations. The authors conducted an extensive analysis of what such a compliance would look like with regard to all data processing principles covered by art. 6 of the DPD. Moreover, they analyzed the notion of ‘data controller light’. This concept was introduced during oral arguments in Google Spain by the Advocate General who asked if it is appropriate to qualify an entity as a ‘controller’ if many of its basic responsibilities are interpreted in a lenient way? The European Commission responded by saying that the search engine’s obligations should be assessed proportionately in light of the specific processing activities. From the data subjects’ perspective, he or she has the right to obtain information with regards to the processing of his or her data (Article 12), the right to object to the processing of the personal data (Article 14(a)), the right to rectification when the data is inaccurate (Article 12) and the right to erasure of his or her personal data when it is inappropriate (Article 12).\textsuperscript{31}

The authors of the paper examined also the ‘right to be forgotten’. The Google Spain case was often referred to in the context of this concept. This ‘right to be forgotten’ will be included in article 17 of the proposed Data Protection Regulation and aims to clarify and strengthen the right of erasure enshrined in article 12 (b) of Directive 95/46. More specifically, article 17 of the proposed DPR would allow data subjects to request the controller to erase their personal data and hinder further dissemination of this data when one of the following grounds applies:

- (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- (b) the data subject withdraws consent on which the processing is based or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

- (c) the data subject successfully exercised the right to object;

- (d) the processing of the data is not in compliance with the Regulation for other reasons.

Since the right to be forgotten is only planned for the future act replacing the Data Protection Directive, the Google Spain case was not decided on its basis. This however did not prevent the CJEU from reaching a conclusion that when requested by the data subject:

> The operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and

\textsuperscript{29} Article 29 Data Protection Working Party, ‘Opinion 1/2008 on data protection issues related to search engines, p. 10.

\textsuperscript{30} CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, c-131/12, 13 May 2014.

\textsuperscript{31} This latest right is one of the key elements in the Google Spain case, as the proposal for the new Data Protection Regulation includes an explicit ‘right to be forgotten’. It would however lead us too far to go into detail regarding this right and its consequences.
containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.32

3.1.2.3. Search Engines and the Freedom of Expression

Search engines facilitate the retrieval of information. Therefore, they should, to a certain extent, be protected by the right to freedom of expression. According to Van Eijk, the activity of making information accessible should be able to claim 'similar status' under article 10 ECHR as the activity of disclosing or disseminating information and ideas.33 With regard to the publication of the search results, Van Hoboken considers that search engines actually produce information (more specifically: information about information). Hence, he sees the activity of the search engines as a separate publication, which deserves independent protection under article 10 ECHR.34 The European Court of Human Rights agreed with these opinions and extended the scope of article 10 to include the means of transmission or reception of information.35

However, even though services of search engines are protected by the freedom of expression, interferences with this right are possible if they are justified in the light of protecting far-reaching rights of data subjects. Moreover, a fair balance needs to be ensured between all the players’ interests. Therefore, the existence of a public interest in information is not enough to justify restrictions on the right to privacy or data protection.36 This position was confirmed by the ECHR in Von Hannover v. Germany. In this case the Court clarified that the publication of photos and articles:

‘the sole purpose of which was to satisfy the curiosity of a particular readership regarding the details of the applicant’s private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.’37

Idle gossip merely serving to satisfy the curiosity of certain readers or viewers and not contributing to any public debate is therefore not protected under the freedom of expression.38

In Google Spain case, the Court decided that when balancing the right to privacy and data protection, with the rights to access information, different factors need to be taken into account. For example, the outcome will be different when an individual plays a significant role in public life:

32 CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, c-131/12, 13 May 2014.
35 ECtHR, Autronic v Switzerland, 22 May 1990; ECtHR, Times v. United Kingdom, 10 March 2009; ECtHR, Open Door v. Ireland, 29 October 1992.
36 ECtHR, Standard Verlags GmbH (n° 2) v. Austria, 4 June 2009.
Whilst it is true that the data subject’s rights protected by those articles [7 and 8 of the Charter of the EU] also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.\(^{39}\)

### 3.2. Media Law

The growing convergence between television and the internet (think of the emergence of ‘over-the-top’ video services, ‘connected TV’, ‘hybrid TV’, ‘social TV’, etc.) and the emergence of new intermediaries that significantly influence people’s media consumption (e.g. search and navigation tools, recommendation services, automated selection tools, etc.) raise fundamental questions with regard to the material scope of contemporary broadcasting laws, both at EU and national level. Some of the video applications developed on the Experimedia platform might come close to resembling traditional TV services. Part of the fundamental legal research carried out in the Experimedia project therefore looked at how broadcasting laws are currently delineated and how this might / should change in the future.

#### 3.2.1. What if Television Becomes Just an App?

The European legislator could hardly foresee the future and rocketing popularity of online video portals like YouTube or Dailymotion when adopting the Audiovisual Media Services Directive (AVMSD). These new and popular media made the European Commission come to the conclusion that we have entered “a new stage in the convergence of Internet and TV”. They urged the European legislator to test the regulatory framework set by the Directive against evolving viewing and delivery patterns.\(^{40}\)

The paper entitled ‘What if Television Becomes Just an App? Re-Conceptualising the Legal Notion of Audiovisual Media Service in the Light of Media Convergence’\(^{41}\) discusses the notion of Audiovisual Media Services.

#### 3.2.1.1. Notion of an Audiovisual Media Service

The aim of the European legislator when adopting the new AVMSD in 2007 was to include every AVMS in their new definition. Article 1 (1) (a) defines an audiovisual media service as “a service as defined by Articles 56 and 57 [ex 49 and 50] of the Treaty of the Functioning of the European Union (1) which is under the editorial responsibility of a media service provider (2) and the principal purpose (3) of

\(^{39}\) CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, c-131/12, 13 May 2014, par. 81.


which is the provision of programmes (4) in order to inform, entertain or educate (5), to the general public (6) by electronic communications networks (7)."  

The seven cumulative criteria of the definition were discussed in the presented paper, and were viewed in the light of the recent online media landscape.

Furthermore, the paper discusses the distinction between linear and non-linear services. Linear services (also referred to as “television broadcasts” in the directive) are video services provided by a media service provider for simultaneous viewing of programmes on the basis of a programme schedule. By contrast, non-linear services are delivered by a media service provider at a moment chosen by the user and at his/her individual request on the basis of a catalogue of programmes selected by the media service provider (on-demand or pull-services).

The so-called graduated regulatory regime in the AVMSD made linear services subject to strict rules whereas non-linear services are only subject to ‘light touch’ regulation. Nevertheless, with the emergence of online video playlists and automated selection tools, the line between these two categories is fading quite rapidly.

3.2.1.2. Convergence and Future Challenges

The article concluded that the lines between services that are regulated by the AVMSD vis-à-vis services that are not is gradually blurring. The authors wondered whether the current definition of AVMS will be enough to encompass the changes in the digital audio-visual media sector. Is the definition still apt to achieve the policy goals – in relation to cultural diversity, protection of minors, prohibition of hate speech, etc. – that the current regulation attempts to pursue?

According to the Green Paper on Media Convergence of the European Commission, automated selection tools and algorithms have a clear potential for empowering citizens, by allowing them to navigate efficiently through today’s information overload and to receive tailor-made services corresponding to their individual needs. But the growing use of these tools will come with major challenges. The role of the media as editors in the public sphere will decrease and the role of platform providers will no doubt strengthen. In order to ensure a fair allocation of responsibilities within the digital media value chain, it is necessary to further explore the nature of selection, filtering and organisation activities of different actors.

42 Article 1(1) (a) AVMSD. The notion also includes audiovisual commercial communication (such as advertising, sponsoring, product placement, etc.).
43 On the condition that they are sufficiently ‘TV-like’, meaning that the non-linear service competes for the same audience as linear television broadcasts, and the nature and the means of access to the service would lead the user to reasonably expect regulatory protection (Recital 24 AVMSD).
44 Article 1, 1 (e) AVMSD.
45 Article 1, 1 (g) AVMSD.
46 The AVMSD motivates this distinction on the basis of the presumed higher impact on public opinion and lower degree of user control in the case of linear services (Recital 58).
3.2.2. Who’s Author, Editor and Publisher in User-Generated Content?

3.2.2.1. The Rise of User-Generated Content and the Role of Platform Providers

The article entitled ‘Who’s Author, Editor and Publisher in User-Generated Content?’ also concerns these changes in the audiovisual media sector and more specifically the growing role of platform providers. It handles the responsibility question for User-Generated Content and the capability of traditional concepts to answer this liability question.

The apparition of User-Generated Content (UGC) is a phenomenon of the Web 2.0 (the read-write web), in opposition to the Web 1.0 (the read only web). The one-way traffic from producers of content to a mostly passive public of Web 1.0 made way for a broad interaction between content producers and more active users. These users participate by commenting and even generating content themselves.

The authors considered that the rise of UGC came with many positive consequences. It leads to a better understanding and cooperation between people and organizations. Moreover, it plays a major role in the democratization of the news process. The traditional media outlets were joined by a diverse array of additional information sources. Furthermore, UGC facilitates social networking and favors the growth of user autonomy while encouraging cultural diversity.

But there are dangers imaginable, especially considering the uncontrolled character of UGC. It could instigate hate speech, privacy invasions, intellectual property infringements, defamation, and child pornography as well as other undesirable content.

Combating this illegal or undesirable content is increasingly difficult as the author is not always known. In such situations, who is responsible for such content? Is the UGC platform provider a mere messenger or does he fulfill a more active role? Is the platform provider the author, editor or publisher of content published online? Moreover, can we use these concepts to define the legal liability for UGC? Mostly for the platform providers, these questions are crucial. Platform providers need to know what is legally required from them. Can they be held responsible for the lawfulness of UGC and the activities of users on their platforms? The presented publication attempted to answer these questions.

3.2.2.2. Degree of Liability of the UGC Platform Providers

It thereby builds further on the study from 2008 on User-Created-Content for the European Commission, in which two models to assess legal responsibility for third party consent were put forward, namely the publisher model and the hosting model. The former, originating from media law and content-related activities, places the full liability for the content that is disseminated on the publisher. The justification is to protect the public’s interest. The hosting model on the other hand relates to technical activities in the context of telecommunications law. It sees liability for third party content as the exception, not the rule.

---

The study found that UGC platform providers “do not fit well into either of the two models. The majority of UCC platforms act in a grey zone between the provision of technical and content-related activities.”

After discussing the conceptual framework for legal liability for UGC, the authors examined relevant case law in a number of EU countries, which shows a considerable lack of consensus in the implementation of liability rules. The authors found that public interest values, such as protection of minors and human dignity, may call for far-reaching liability for third party content. Very often, there is no other way for the injured parties than to take action against the intermediary, whenever the real author remains unknown. At the same time, the authors point to several risks attached to this approach. Making UGC platform owners liable for content disseminated through their platforms might result in excessive censorship by these providers out of fear for prosecution. Moreover, making them liable for the illegal and harmful content could expose them to an excessive financial, technical and legal burden, which will often be disproportionate. Also, they might have to infringe privacy rules when revealing the identity of the real author of illegal or harmful content. All of these conflicting interests make finding the right balance quite difficult.

In our article, we have provided an update of the relevant case law and introduced a further distinction in the publisher model – differentiating between liability for print publications on the one hand and for audio-visual content on the other hand. The conclusion remains that there are divergent approaches in Europe and that a harmonised approach would be welcome to increase legal certainty for actors that operate in multiple Member States.

3.3. Conclusion
The legal research conducted in the EXPERIMEDIA project focused on the new types of services. Legal issues presented by these types of services very often extend the scope of FMI. For this reason the conducted legal research analysed concepts that are generally applicable to the emerging technologies.

A great amount of the presented fundamental legal research in EXPERIMEDIA focused on search engines as an example of new type of services. Even though search engines, strictly speaking, are not that new in the online services landscape, they continue to provide challenging legal questions. Only recently, in the Google Spain judgment, their position as data controllers within the scope of the European data protection law has been confirmed. The conclusions of the legal analysis of search engines are not limited to these services and can serve as analogy for other new types of services.

The new types of services present new lacunae in the legislation that need to be addressed. For example, legislators should acknowledge that new forms of content delivery and production (e.g. UGC) require specifically adapted regulation. The same applies with regard to processing of personal data by the new types of services and their liability for third party content. The current regulation is insufficient to adequately regulate all these questions. This creates a situation of legal uncertainty which might hinder further development of the new types of services.

Moreover, it is also clear from the discussion that freedom of expression is often an issue that is overlooked in the balancing of rights. The protection of privacy and data protection cannot be in disregard of the fundamental right to the freedom of expression. This debate transcends the traditional barriers between the sector-specific regulatory frameworks.

On the basis of these findings, as well as the observations made when assisting partners in legal compliance we provide a list of policy recommendations. The articulated recommendations relate to the processing of personal data, the legal grounds for processing in the context of scientific research and an awareness of the convergence of the various media services and their influence on the freedom of expression.
4. **Policy Recommendations**

In this section of the deliverable several policy recommendations are presented. These recommendations are based on the lessons learned from the fundamental and applied research conducted in the EXPERIMEDIA project. Problematic areas will be addressed via specific recommendations aimed at certain stakeholders: policy makers, researchers in the EU research programmes or experimenters conducting experiments in the area of FMI. The main goal is to share the experiences gathered throughout the project and to raise awareness of the relevant stakeholders.

4.1. **Privacy and data protection**

4.1.1. **Responsibility for Processing Personal Data in Research Projects**

Compliance with data protection regulations of several countries was one of the major tasks of the legal partner in EXPERIMEDIA. Assisting project partners in fulfilling their formal obligations was a task that had to be repeated for each round of experiments. The technical details needed to be specified to decide on these issues, and it took some time to fill in the administrative side in each country and consult the various Data Protection Authorities. These difficulties occurred in most FP7 research projects. The structure of the European research projects doesn’t coincide with the general division of roles between the data protection actors. It can be very difficult to define the responsible party for the processing of personal data because several actors are involved in the design of the system or participate in the experiment. This issue of accountability should be attended in order to make every project partner aware of their role within the project. Especially with something as delicate as the processing of personal data, properly assigned roles are crucial. This issue should be addressed by the EU researchers and monitored by the European Commission.

**Recommendation:** the definition of roles and privacy issues should be taken care of in the beginning of the project.

Furthermore, the legal and ethical implications of the processing of personal data should be given sufficient weight in the project structure by the project partners. In EXPERIMEDIA the core partners organized legal tutorials for the new partners joining through the Open Calls. It proved very beneficial to all the involved parties. With this formalized approach, agreements on the necessary aspects of the processing will prove easier and more transparent.

**Recommendation:** workshops and tutorials dealing with legal aspects of projects should be organized to ensure good understanding of the relevant issues.

4.1.2. **Legal Ground for Processing Personal Data in Research Projects**

The choice of the appropriate legal ground can influence the entire course of a project. After all, according to the European legislation data controllers are not exempt from the requirement of having a legitimate ground for processing of data if the personal data is made public by the data subject. Article 7 of the Data Protection Directive provides only 2 grounds that can be used by controllers of personal data in a research project: consent of the data subject and legitimate
interest of the controller. Unfortunately, both these grounds come with significant issues. Consent might be quite difficult to achieve in projects that want to extract (publically available) data from Social Networks. Unless an experiment is targeted at a small group of users, asking all the Social Network users for their consent is simply not possible.

This leaves us with the second ground foreseen in the Data Protection Directive, i.e. the legitimate interest of the controller. This ground allows for processing of personal data on condition that in the pursuit of his interest the controller cannot override the fundamental rights of the data subjects (such as for example right to privacy). However, the meaning of this condition is still very much under debate in the different Member States. Only in the recent Google Spain judgment by the CJEU this legal ground was confirmed as valid for the data processing operations of search engines. This however, does not answer the question whether scientific research interest could prevail over the rights of individuals.

It would therefore be laudable to include a general exception from the data protection obligations when the processing takes place within the context of scientific or research projects. To prevent abuse, such processing ground should be limited only to the duration of the project. In the currently debated Data Protection Regulation, that should replace the Directive, such exception has been proposed. It is to be seen if it makes it to the final version of the act.

Recommendation: the EC should consider introduction of ‘scientific research’ as a legal ground for processing of personal data.

4.1.3. Transparency

Transparency should always be a priority in projects such as EXPERIMEDIA that involve experiments with volunteers and processing of their personal data. Clear and unambiguous information should be provided to all interested parties. Participants have to be informed about the details of the experiments, who conducts them and for what purpose. They need to know which types of their data will be used, for how long and whether it will be forwarded to anyone else. They should also be informed who they could contact if they have any additional questions, or would like to exercise their rights (e.g. right to erasure). This information should be provided to them in a consent form and/or privacy notice. Depending on the type of experiment, a clear Privacy Policy and well developed Terms and Conditions might be required. Fairness and transparency should be considered a basic requirement for research projects in order to build confidence of the participating individuals and ensure trusted relationships with them.

Recommendation: researchers and experimenters should ensure the adequate level of transparency of their activities towards the participants and data subjects.

4.2. Intermediary Liability

4.2.1. Situation of Search Engines

Search engines are a new type of service providers that has not been sufficiently addressed by the lawmakers. They do not fall within any of the three categories of services for which the E-Commerce Directive provides liability exemptions. This lack of regulation at EU level for the services of search engine providers leads to legal uncertainty and fragmentation. Article 21 of the
Directive announced a re-evaluation of the issues concerning information location tools (search engines) after the first report on the implementation of the Directive. However since 2001, the re-evaluation has not been set in motion. Therefore, especially considering the technological developments since 2001, the situation of search engines with regard to liability for third party content should be reassessed at the EU level.

**Recommendation: the EC should address the situation of search engines as a new type of intermediary service providers.**

The current review of the E-Commerce Directive seems like an excellent opportunity to do this reassessment. New rules on the services of search engines could ensure these preset goals, i.e. to reduce legal uncertainty by amending the liability exemption rules in the E-Commerce Directive. A move towards this objective was already present in the two consultations on the E-Commerce Directive and the Notice and Action but results are still to be seen.

### 4.2.2. Safeguards for Freedom of Expression in the Notice-and-Take Down mechanism

The second recommendation refers to the freedom of expression and the risk of private censorship while implementing the E-commerce Directive. Article 14 of the E-commerce Directive describes the conditions for exempting hosting providers from liability for the third parties content. This provision is a framework for a notice-and-take down procedure, a mechanism that can be used to enlist hosting providers in eliminating infringing content from the Internet. In practice this mechanism entails that hosting providers are not obliged to actively monitor content on their servers, but are compelled to react upon obtaining knowledge about illegal activities on their server. If they don’t react, they lose the immunity set out in the Directive.

The Directive does not specify what this notification should look like or what information it should include. It also does not specify what the required reaction time is. Most Member States decided to transpose the article verbatim, leaving these issues unattended. This means that many of the EU countries do not have a specific procedure for hosting providers’ removal of online content. This increases the risk of private censorship considerably. Putting intermediaries in a situation where they have to quickly decide about legitimacy of content to avoid liability creates an incentive to take down content regardless of its nature. Systematic removal of content without its proper analysis poses a threat to freedom of expression online.

**Recommendation: safeguards should be introduced at the EU level to prevent interference with Freedom of Expression.**

These concerns should be taken into account in the on-going review of the E-commerce Directive. The outcome of the review should provide minimum guidelines for taking down content. This procedure should be harmonised at the EU level to ensure that safeguards for the freedom of expression are the same across the EU.
4.3. Media Law

The last recommendation is related to the blurring line between services that are regulated by the AVMS Directive and services that are excluded from its scope. In today’s media landscape, the distinction between traditional broadcast services and new online video services decreases, while at the same time new intermediaries enter the traditional value chain for audiovisual content.

In its Green Paper on Media Convergence, the European Commission aimed to trigger the debate on how to delineate the next generation of audiovisual content regulation on Europe and launched many questions that need to be discussed in the coming years. Should future media laws continue to distinguish between print and audiovisual media, or treat them alike? Should it include navigational tools and other new intermediaries? Should it roll back existing rules for providers currently covered by the Audiovisual Media Services Directive? Should it specifically include measures that aim to guide users of media services towards their specific individual needs via filtering and personalisation mechanisms? What are the technological solutions to ensure traditional public policy values (such as cultural diversity, protection of minors, media pluralism, etc.) and should they be enforced via binding rules? What will be the impact of the increasing use of personal filtering and selection activities on public opinion formation – will it undermine the creation of a ‘public sphere’ through the media, and if so, should this be remedied through legal measures? Will the media consumer in the future pay more and more with personal data, and if so, what will this imply for democratic access to information?

In the context of this project, we provided original analysis on the growing decision practice of national media authorities on delineating the concept of ‘audiovisual media service’, and we carried out a literature review on some of the other questions, e.g. on the (legal) role of search and navigation tools. But several questions remain in the area of analysing the changing notion of audiovisual media services and enforcing policy goals in an ever more global digital media environment. Furthermore, due to this rapidly changing media environment, research within this area should be constantly (internally or externally) reviewed and updated to ensure compatibility with the latest techniques and changes in the media landscape.

The notion of ‘audiovisual media service’ is evolving quickly due to the convergence between print media and audiovisual media, on the one hand, and television and the internet, on the other hand. As the approach by national media authorities differs, this is resulting in regulatory divergence and, hence, legal uncertainty within the European internal market. Also the rise of new intermediaries (in particular online platforms, OTT providers, and navigational tools) that take up an important role (and that attract a growing percentage of advertising revenues) in the traditional value chain forces policy makers to rethink the boundaries of existing media laws.

Recommendation: Further research is needed in particular on the role that technology can play in ensuring traditional policy objectives (such as cultural diversity, protection of minors and media pluralism), and to what extent this may imply rolling back existing obligations on the traditional market players.
5. Conclusion

The EXPERIMEDIA project provided a great opportunity for interesting legal analysis. It allowed for examination of legal questions in numerous areas, such as privacy and data protection, intermediary liability and media law. All these aspects of the project have been researched thoroughly to ensure compliance of EXPERIMEDIA with the European legal framework.

Legal analysis conducted in EXPERIMEDIA by the legal partner KU Leuven consisted of two types of research: fundamental and applied. The former consists of examining relevant legal questions in order to enhance knowledge on legal and regulatory requirements. The overall goal of this type of analysis is to bring new insights to improve the law making process related to the three areas of law in EXPERIMEDIA as well as FMI. In this project specifically, KU Leuven focused on questions relating to allocation of responsibility for processing of personal data between controllers and processors in new types of services, right to be forgotten, balancing of freedom of expression and right to privacy, liability for UGC, Notice and Action initiative, or the two-tiered approach of the AVMS Directive.

To achieve this objective KU Leuven engaged in writing scientific publications and presented them at international conferences and workshops. The results of this research were summarized in the presented deliverable.

KU Leuven conducted also a vast amount of applied research in EXPERIMEDIA. This type of research consisted of providing legal and ethical oversight to the project partners and guiding them to compliance with the applicable laws, such as data protection law. This task is aimed to ensure that the project as a whole, and in particular partners, do not infringe upon any rights or regulations. Moreover, the assistance of a legal partner who attends to these issues from the beginning of the project is recommended to lower the costs of regulatory compliance of the developments.

Based on the lessons learned from these two types of research, KU Leuven developed a list of policy recommendations in the areas relevant to EXPERIMEDIA. This list was presented here in Section 4.