Deliverable D5.1.5 is a second iteration of the analysis of the legal and ethical framework for the deployment of EXPERIMEDIA testbeds. It continues and extends the analysis conducted at the beginning of the EXPERIMEDIA project in deliverable D5.1.2. This deliverable focuses on the main legal developments in three areas: privacy and data protection, liability of internet intermediaries and media law. Additionally, it addresses the issue of compliance with terms and conditions for API by application developers.
<table>
<thead>
<tr>
<th><strong>Project acronym</strong></th>
<th>EXPERIMEDIA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full title</strong></td>
<td>Experiments in live social and networked media experiences</td>
</tr>
<tr>
<td><strong>Grant agreement number</strong></td>
<td>287966</td>
</tr>
<tr>
<td><strong>Funding scheme</strong></td>
<td>Large-scale Integrating Project (IP)</td>
</tr>
<tr>
<td><strong>Work programme topic</strong></td>
<td>Objective ICT-2011.1.6 Future Internet Research and Experimentation (FIRE)</td>
</tr>
<tr>
<td><strong>Project start date</strong></td>
<td>2011-10-01</td>
</tr>
<tr>
<td><strong>Project duration</strong></td>
<td>36 months</td>
</tr>
<tr>
<td><strong>Activity 5</strong></td>
<td>Legal, sustainability and promotion</td>
</tr>
<tr>
<td><strong>Workpackage 5.1</strong></td>
<td>Legal, ethical and regulatory framework</td>
</tr>
<tr>
<td><strong>Deliverable lead organisation</strong></td>
<td>ICRI-KU Leuven</td>
</tr>
<tr>
<td><strong>Authors</strong></td>
<td>Aleksandra Kuczerawy (ICRI-KU Leuven), Jeroen Verschakelen (ICRI – KU Leuven), Yung Shin (Marleen) Van Der Sype (ICRI-KU Leuven), Peggy Valcke (ICRI – KU Leuven)</td>
</tr>
<tr>
<td><strong>Reviewers</strong></td>
<td>Remi Francard (FDF), Sandra Murg (JRS)</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.01</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Final</td>
</tr>
<tr>
<td><strong>Dissemination level</strong></td>
<td>PP: Restricted to other programme participants (including the Commission)</td>
</tr>
<tr>
<td><strong>Due date</strong></td>
<td>PM18 (2012-04-30)</td>
</tr>
<tr>
<td><strong>Delivery date</strong></td>
<td>v1.0: 2012-05-14; v1.01: 2013-05-17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Version</strong></th>
<th><strong>Changes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial release</td>
</tr>
<tr>
<td>1.01</td>
<td>Changed dissemination level from PP to PU</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Executive Summary ................................................................................................................................. 4
2. Introduction .................................................................................................................................................. 5
3. Final general ethical and legal framework ................................................................................................. 6
4. Application of the general ethical and legal framework on the deployment of the EXPERIMEDIA testbeds .............................................................................................................................................. 8
   4.1. Data Protection Directive 95/46/EC ........................................................................................................... 8
       4.1.1. Definition of personal data .................................................................................................................. 8
       4.1.2. Notification ........................................................................................................................................ 11
       4.1.4. Proposal overview ............................................................................................................................. 13
       4.1.5. Consequences of the reforms in the area of privacy and data protection for FIRE and similar developments .......................................................................................................................... 15
   4.2. E-Commerce Directive 2000/31/EC ......................................................................................................... 16
       4.2.1. Liability of Intermediaries .................................................................................................................. 16
       4.2.2. Review of the E-Commerce Directive ............................................................................................... 19
       4.2.3. Notice-and-Action Initiative ................................................................................................................ 19
       4.2.4. Consequences of the reforms in the area of liability of intermediaries for FIRE and similar developments .......................................................................................................................... 22
   4.3. AudioVisual Media Services Directive .................................................................................................. 23
       4.3.1. Green Paper on AudioVisual Media Services ..................................................................................... 23
       4.3.2. Green Paper on convergence ............................................................................................................. 25
       4.3.3. Consequences of the reforms in the area of media law for FIRE and similar developments ............... 26
5. Terms and Conditions for API developers ................................................................................................. 27
   5.1. Introduction ............................................................................................................................................ 27
   5.2. Relevance of the API T&C’s ................................................................................................................. 28
   5.3. Compliance with the API T&C’s ............................................................................................................ 31
   5.4. Preliminary conclusion .......................................................................................................................... 32
6. Conclusion .................................................................................................................................................... 34
1. Executive Summary

Deliverable D5.1.5 is a second iteration of the analysis of the legal and ethical framework for the deployment of EXPERIMEDIA testbeds. It continues and extends the analysis conducted at the beginning of the EXPERIMEDIA project in deliverable D5.1.2 “Initial legal and ethical framework for the deployment of EXPERIMEDIA testbeds”. In Section 3 this deliverable provides a final list of the applicable legal framework for EXPERIMEDIA. Further on, the present deliverable focuses on the main legal developments in three areas most relevant for the project. These areas include: privacy and data protection, liability of internet intermediaries and media law. These new developments are addressed in Section 4 of the deliverable. Section 4.1 focuses on the main issues in privacy and data protection that are present in EXPERIMEDIA. It also describes the current state of works and accompanying discussions on the review of the Data Protection Directive 95/46/EC. A proposal of a new regulation has been published at the beginning of 2012 and since then the works are on-going. In Section 4.2 the review of the e-Commerce Directive 2000/31/EC is addressed. The works in this case are less developed since no official proposal has been published so far. Section 4.3 describes the new developments in the area of Media Law. It focuses on two Green Papers: on the online distribution of audiovisual works in the European Union and Green Paper on Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values. The latter document has been adopted by the European Commission very recently, which means that only initial analysis has been conducted.

Section 5 of the present deliverable addresses the issue of compliance with the developers Terms and Conditions for API. This matter is extremely important for developers of applications built on top of existing platforms or software, for example Social Networking Sites (hereinafter SNS). Compliance with the rules laid down by such platform providers can be problematic, for several reasons that are further described below.

Finally, the present deliverable ends with conclusions in Section 6.
2. Introduction

EXPERIMEDIA develops and operates a unique facility that offers researchers what they need for large-scale Future Media Internet experiments. Experiments within the EXPERIMEDIA project are expected to explore Future Internet systems targeting enhanced and contextualised user experience, immersive and interactive media technologies, content production, distribution and delivery platforms, and new social interaction models. With such an objective a number of legal questions arise.

The aim of this deliverable is to describe the final legal framework and to evaluate the consequences for the EXPERIMEDIA project. Besides, it will identify problems that could be encountered due to the current state of the regulatory framework and describe the on-going review process of the several applicable policy documents and the accompanying discussions. This deliverable focuses on three areas, namely the Privacy and Data Protection (Data Protection Directive 95/46/EC), Liability of Intermediaries (E-Commerce Directive 2000/31/EC) and Media Law (Green Paper on the online distribution of audiovisual works in the European Union and Green Paper on Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values). The deliverable also addresses the issue of compliance with API Terms and Conditions for developers. This is an extremely relevant issue in the context of FIRE and Internet of Services. Every application that is build on top of the existing platforms or software must comply with such platform’s rules on accessing its content. These rules can be very restrictive and difficult to comply with, especially by developers who want to access such content for free. There are several reasons why compliance can be problematic and they will be described below in this deliverable.
3. Final general ethical and legal framework

Since the emphasis of this deliverable lies more in what is important for the experiments, rather than to provide a complete overview of the legal framework within the EXPERIMEDIA project, it will suffice here to provide only a short summary of the legal rules found in D5.1.2 Ethical, legal and regulatory framework for social and networked media (Annex 1):

- **Media regulation:**

- **Intellectual property rights regulation:**
  - Directive 2006/115/EC of December 12, 2006 on rental right and lending right on certain rights related to copyright in the field of intellectual property, O.J. 2006 L376/28;
  - Directive 93/83/EEC of September 27, 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable transmission;

- **Data protection regulation:**
  - Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L281/31;
  - Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

- **Liability of Intermediaries**
  
  - Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

This deliverable will focus on new developments in the areas of data protection and privacy, liability on intermediaries and media regulation. It will be presented on the basis of the on-going reviews of the Data Protection Directive 95/46/EC, E-Commerce Directive 2000/31/EC and the Green Paper on the online distribution of audiovisual works in the European Union, also a new Green Paper on Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values.
4. Application of the general ethical and legal framework on the deployment of the EXPERIMEDIA testbeds

Within Europe, the right to privacy can be found in Article 8 of the European Convention on Human Rights, which concerns the protection of the private and family life, home and correspondence of the citizen. This article has been later enforced by other regulatory instruments at the level of the European Union. Apart from Directive 95/46/EC, the EU has also provided for privacy protection in the field of electronic communications (Directive 2002/58/EC) and in the field of data retention (Directive 2006/24/EC). Besides, the EU has included the right to privacy, as well as the right to data protection, in the Charter of Fundamental Rights of the European Union, anchoring the value of human rights protection in the Treaty on the European Union.

4.1. Data Protection Directive 95/46/EC

During the first year of the EXPERIMEDIA project it became clear that there were two specific issues that required a more thorough approach. These specific issues, regarding the definition of personal data and regarding the notification, will be clarified in the following paragraphs.

4.1.1. Definition of personal data

**Definition.** Article 2(a) Directive 95/46/EC defines ‘personal data’ as: “...any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

**Scope of the definition.** Note that the directive does not distinguish between written, oral, visual or any other type of information. Furthermore, the information needs to identify a natural person or make this person identifiable. A person can be considered as being identified when his identity can directly be established. This is the case when using a national single identification number of general application. As such an identification number is uniquely assigned to every single citizen; this citizen can be **directly identified** using this identification number. Other examples include name, address, date of birth, etc. While these last examples are not necessarily unique for one single citizen, they carry a high probability of direct identification of the person involved. If the person involved cannot be identified directly, he may still be **identified indirectly** by combining different elements or by deducing other identifiers from available

---

3 O.J. C 83 of 30 March 2010, 393.
4 For a full overview of the existing European privacy regulation see D5.1.2, 34-56.
5 A national single identification number of general application is an identification number attributed by States to their citizens in order to uniquely identify them. Such identification numbers are used in, for instance, Belgium, Sweden and Spain.
information. In such case, the person is identifiable. This definition leads to a very broad spectrum of information that could potentially serve as personal data.⁶

**Limits of the concept personal data.** As the definition of the concept of personal data in the directive has a very broad scope, its precise interpretation appears to differ amongst Member States. Aiming to provide a more coherent interpretation across the EU, the Article 29 Working Party adopted an opinion on the concept of personal data.⁷ As this concept forms the very basis of the EU legal framework on data protection, a coherent and homogenous interpretation by all Member States is of utmost importance. Although it could be argued that the definition of the concept of personal data has deliberately been formulated in a broad manner in order to embed flexibility in the application of the concept to various circumstances, it should also be noted that the scope of the concept should not be overstretched.⁸ Here, the Working Party clearly states that it would be undesirable to stretch the existing concept for application to situations not intended to be covered by the legislator. This seems to be an appropriate reaction as the idea of overstretching the applicability of existing concepts is one of the core issues that augmented the demand for review of the directive. However, the Working Party also warns for a too narrow application of the directive. When the application of the concept of personal data may at first sight seem to be over stretched, one should first look at the scope of the directive, in particular article 3. Next, one should look at exemptions or simplifications in the directive or in national implementations thereof. The Working Party addresses the national Data Protection Supervisory Authorities (DPA) to monitor the application and interpreting of the directive and to endorse a broad definition of concepts for application of the directive to societal and technological evolutions.

1) The Working Party continues its opinions by analysing the constitutive elements of the concept of personal data. First, the element of information is analysed.⁹ Here, it is indicated that nature and content of the information are of no importance as all information is included under the scope of the directive, regardless of nature or content. From this, one can deduce¹⁰ that the directive is not limited to the protection of information regarding the strict sphere of home and family, but also touches subjects beyond this sphere such as labour law¹¹, court records¹² and direct marketing¹³. Also the format or medium used in presenting the data is of no importance.

2) Second, the information needs to relate to an individual.¹⁴ This can be a direct relation, where information about a person is given.¹⁵ Also possible is an indirect relation, whereby information is provided on an object that relates to the individual.¹⁶ In short,

---

⁶ Deliverable D5.1.2, p. 35.
⁸ Ibid.
⁹ Ibid.
¹¹ Article 8 (2) (b) Directive 95/46/EC.
¹² Article 8 (5) Directive 95/46/EC.
¹³ Article 14 (b) Directive 95/46/EC.
¹⁵ The Working Party lists medical and personnel records as examples of files in which data relating to an individual can be found.
¹⁶ The value of a house can, for instance, give information on the assets and wealth of its owner.
the Working Party considers data to relate to an individual if “it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated”.\textsuperscript{17} According to the Working party, information can relate to an individual if there is a content element\textsuperscript{18}, a purpose element\textsuperscript{19} or a result element\textsuperscript{20}.

3) Third, regarding the element of identified or identifiable individuals,\textsuperscript{21} the Working Party notes that this means that the \textit{individual should be distinguished} from the other members of the group, or that it should be possible to do so. \textbf{Directly} or \textbf{indirectly} refers to the degree of precision by which a certain identifier can indicate a single individual.\textsuperscript{22} For indirect identification, one will have to combine several elements of information together before a unique identification can be made. For defining the notion of identifiable, the Working Party refer to recital 26 of the Directive where identifiable is defined as all the means likely reasonably to be used to identify an individual. By determining what is likely reasonably to be used one, has to keep in mind several factors – such as the cost of identification – and reality has to be applied. Hypothetical possibilities for identification are not likely reasonably to be used and are therefore not to be considered as personal data. The Working Party also makes note of the use of pseudonymization of data to disguise identities and of anonymization to make identification impossible.

4) The last element analysed by the Working Party is that of the \textit{natural person}.\textsuperscript{23} As explained earlier, the directive protects the rights and freedoms of natural persons. In this opinion, the Working Party elaborates on the fact that this data is generally regarded to relate to living natural persons. Therefore, two particular cases could come to mind: the dead and the unborn.

5) In general, the \textbf{dead} are no longer regarded as being part of the concept of natural persons and are therefore excluded from data protection rights. Exceptions to this rule may, however, apply. For one, if the controller is not certain of a person’s death, he will process data relating to that person as if he were living. Data relating to the dead may also provide information on the living, for instance hereditary medical conditions, and is therefore to be processed according to the applicable provisions in the directive. Regarding medical data it should also be noted that confidentiality duties continue even after death.

6) Although most, if not all, Member States have reached consensus on the \textbf{end of life}, there are still differences in national legal systems on the beginning of life, complicating the case of personal data relating to the unborn. One will have to look into the national provisions on rights relating to the unborn in order to establish whether a particular State grants data protection rights to this case.

\textsuperscript{18} If information on an individual is given, regardless of any specific purpose.
\textsuperscript{19} When data is provided for a specific use.
\textsuperscript{20} When the data provided can have an impact on an individual’s rights and interests.
\textsuperscript{22} This is obviously a contextual matter. The notion “man in business suit” may not provide much help for identifying a particular individual on Wall Street, while it may be useful to single out someone in a more rural crowd.
7) Note that, if certain data appears not to be personal data under the scope of the directive, one might have to look at national implementation thereof as these may have enlarged the scope of the directive. The pending review of the directive may also have implications to the precise scope of the concept of personal data.

8) With these analyses of the core notions of the concept of personal data, the Article 29 Working Party hopes to have cleared the precise scope of this foundation of the EU legal framework on data protection.\(^{24}\)

**Personal data in the project.** The researchers within the EXPERIMEDIA project tried to avoid the use of personal data as much as possible. Where the gathering of personal data could be avoided, no personal data was gathered. Where the storage of personal data could be avoided, no personal data was stored. To determine which data has to be considered personal, the opinion of the Working Party was taken into consideration.

**Anonymization of personal data.** Besides, the researchers tried to anonymize the personal data, which was unavoidable to gather. During the first half of the project, it became clear that researcher often think that they anonymized personal data, although this is not accurate from a legal point of view. From a legal point of view, personal data is only being anonymized when this anonymization is being irreversible. This means that there must be no possibility to go back and de-anonymize the data in such a way that these individuals may be identified/identifiable again. At the current state of development, however, it seems that a full anonymization, with a 100% guarantee is not achievable. Developers admit that there cannot be a perfect assurance that de-anonymization will not be (eventually) possible. This means that the legislation on protection of personal data continues to apply.

### 4.1.2. Notification

Another issue, which was extensively discussed in the EXPERIMEDIA project, was the notification of the data protection authority. It should be noted, that this issue seems to be problematic in many European research projects, due to their specific character.\(^{25}\)

**General rule.** In order to assess whether a certain processing complies with the principles set forth by the directive, a duty of notification has been included in Article 18 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Member States can, however, simplify the notification or provide exemptions for a number of reasons listed under Article 18 (2). Most notably, this includes the appointment of a personal data protection official.

Regarding the content of the notification, Article 19 states that this includes:

(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the processing;
(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

\(^{24}\) D5.1.2, 36.

\(^{25}\) See more on this topic FP7 SocIoS project, deliverable D6.6 Legal Evaluation and Recommendations.
(d) the recipients or categories of recipient to whom the data might be disclosed;
(e) proposed transfers of data to third countries;
(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

The Member States must also determine which type of processing can bear specific risks for the personal rights and freedoms and must ensure that these types of processing are examined prior to their start. The national supervisory authority will perform such examination.

Finally, the Member States need to adopt measures to guarantee the publicity of the processing operations. National supervisory authorities will keep a public register of duly notified processing operations. Also processing operations exempt from the duty of notification need to supply the information included in Article 19.

**Regulation in the EXPERIMEDIA testbed Member States.**

- **Austria:** whenever notification is required this should be done on the basis of the Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000), with the national data protection authority of Austria, namely the Austrian Data Protection Council;
- **Spain:** whenever notification is required this should be done on the basis of the Organic Law 15/99 of 13 December 1999 on the Protection of Personal Data and Law (Ley Organica), with the national data protection authority of Spain, namely the Spanish Data Protection Agency;
- **Greece:** whenever notification is required this should be done on the basis of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended by Laws 2819/2000 and 2915/2000, with the national data protection authority of Greece, namely the Hellenic Data Protection Authority.

In the EXPERIMEDIA project the issue of notification to the data protection authorities is a recurring problem. This is because in EXPERIMEDIA there are a number of experiments, with different purposes and objectives, and they are run by different project partners. This means that during every Open Call specific analysis for each experiment is required to answer the question about which entity is a data controller, whether there is a need to notify the relevant DPA and what should be the adequate description of the processing activities in particular experiments.

**4.1.3. Review of Directive 95/46/EC – on-going reform**

On 25 January 2012, the European Commission proposed a comprehensive reform of the European Data Protection Directive of 1995, which is no longer adequate in the light of technological process and social development.

---

In this deliverable this proposal will be discussed. It will be indicated how these legal changes could be of relevance for the EXPERIMEDIA project. Key subject of analysis is the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data\(^29\) (General Data Protection Regulation). After an overview of this new legal document, some comments on the new proposal will be formulated in the last paragraph of this section.

Nevertheless, it has to be emphasized that the discussed document is only a proposal. It is currently in the centre of heated discussions, results of which are difficult to foresee. Every part in it may be modified or removed in the future. For this reason a detailed analysis of the consequences of the discussed proposal for the EXPERIMEDIA project as a whole, and specific experiments in particular, seems to be a premature attempt.

4.1.4. Proposal overview

**EXPLANATORY MEMORANDUM.** The text of this proposal starts with an explanatory memorandum which explains the context of the proposal, the results of consultations with the interested parties and impact assessment, the legal elements of the proposal and the budgetary implication of the proposal.

According to this explanatory memorandum, rapid technological developments and globalisation have brought new challenges for the protection of personal data. Through social network sites, cloud computing, location-based services and smart cards, the scale of data sharing and collecting increased dramatically. Such types of technology allow private companies as well as public authorities to use personal data on an unprecedented scale in order to pursue their activities. All this has transformed both the economic and social life of individuals. In this ‘brave new data world’ we need a robust set of rules, which will be provided by this proposal for regulation.

**THE PROPOSAL.** Hereunder a list of the major changes in the proposal is provided\(^30\):

1) The proposal aims to set up a regulation instead of a directive. In this way there will be only one single piece of legislation on data protection applicable across the whole European Union. In contrast to a directive, a regulation is a binding legislative act. Therefore it must be applied in its entirety by all EU Member States. A directive, on the other hand, only sets out a goal that the EU Member States must achieve, whilst letting the Member States choose how. A regulation provides therefore more certainty and aims for more harmonisation than a directive and is that way more desirable for the regulation of data protection in Europe;

2) The proposal aims to provide the data subjects with a ‘right to be forgotten’. This right to be forgotten will help individuals to better manage online data-protection risks. When an individual no longer wants his/her data to be processed, and there are no legal

---


grounds for retaining it, the data will be deleted. Nevertheless, it should be clear that this right is about empowering people and not about erasing past events or restricting the freedom of the press;

3) The proposal states that whenever consent is required for the processing of their personal data, this consent will have to be given explicitly, rather than only to be assumed;

4) The proposal aims to provide the data subject with easier access to his/her own data and the freedom to transfer his/her personal data from one service provider to another (right of data portability);

5) The proposal states that companies and organisations will have to notify serious data breaches to the data subjects as well as to the relevant data protection authority without undue delay, even within 24 hours when feasible;

6) The proposal aims to provide more transparency about how personal data is handled, with easy-to-understand information, especially for children;

7) The proposal states that companies will only have to deal with a single national data protection authority (single point of contact), even when their personal data is processed outside their home country. This means that only one single data protection authority will be responsible for a company, even when this company is operating in several countries (one-stop-shop). This will be the data protection authority where the company has its main base;

8) The proposal aims for an enhanced cooperation between data protection authorities on cases with a wider European impact, to ensure the consistent application of rules across the European Union;

9) The proposal gives individuals the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country;

10) The proposal provides clear rules on when EU law applies to data controllers outside the EU. This means that the EU regulation may also apply to companies not established in the EU, if they offer goods and services in the European Union or monitor the online behaviour of citizens;

11) The proposal aims to increase the responsibility and accountability for those processing personal data. Therefore the proposal requires that companies with more than 250 employees should be proactive and take measures to ensure compliance with the data protection law by appointing a data protection officer;

12) The proposal also introduces the principles of ‘privacy by default’ and ‘privacy by design’ to ensure that individuals are informed in an easy and understandable way about how their data will be processed;

13) The proposal states that unnecessary formalities and other administrative and/or bureaucratic burdens and requirements, such as the notification requirements for companies processing personal data, will be removed (simplification of the regulatory environment);

14) The proposal also states that transfers of data outside the EU should be simplified, while ensuring the protection of personal data.

15) Finally, the proposal states that the national data protection authorities will be strengthened so they can better enforce the EU regulation at home.
4.1.5. Consequences of the reforms in the area of privacy and data protection for FIRE and similar developments

If the new Data Protection Regulation would be adopted in the way it is stated in the proposal, some current issues would be outpaced whilst new issues will arise. In this paragraph it is aimed to overview the changes which are legally relevant for the EXPERIMEDIA project and FP7 researchers in general. The main developments, in the context of EXPERIMEDIA are considered to be:

- Right to be forgotten for social networks.
- Notifications and other bureaucratic burdens will be removed.

It should be highlighted that it is not very likely that the new Regulation will enter into force before the end of the EXPERIMEDIA project. Moreover, as was pointed out earlier, the proposal is still being discussed by the stakeholders, which means that the final version of the Regulation is still to be provided. For these reasons the possible consequences for specific experiments are not described in details. The impact of the proposal is rather evaluated for FIRE research in general.

Right to be forgotten for Social Networks

Social networks are of a big importance for the EXPERIMEDIA project. In Schladming, social networks are for example used to support a smooth and satisfactory customer journey. This makes it eligible to provide an overview of how the right to be forgotten most likely will affect social networks.

The implementation of a right to be forgotten in the context of social networks will however not be an easy matter. It has been argued that it would be simply impracticable to create such a right, e.g. because data may have been copied (transferred) to another social network already, or because data may have been anonymized. In other words, instances of “secondary use” of personal data might render a “right to be forgotten” ineffective in practice. Moreover, technological means for implementing such a right are a necessary but not a sufficient condition. Through the use of meta-tags, an “expiry date” may be applied to personal data, causing the information to disappear automatically after a given period of time. However, such technological solutions would still have to go hand in hand with laws enforcing compliance. Likewise, technologies similar to digital rights management (DRM) could be used to implement a right to be forgotten, but such measures would have to be accompanied by anti-circumvention laws.

Hence, it becomes clear that the implementation of a “right to be forgotten” in the context of social media would require considerable efforts on the part of social network providers, both on a technical and on a (legal) compliance level.

Notifications and other bureaucratic burdens

As mentioned before, according to Article 18 of the Data Protection Directive data controllers have an obligation to notify the relevant Data Protection Authorities about activities involving
processing of personal data. This refers as well to processing of personal data conducted in the framework of research projects, as there is no exemption for such purpose in the Directive.

Under the new regulation this will no longer be the case. One of the main goals of the proposal was to abolish unnecessary administrative obstacles. Under the new Regulation businesses and organisations will only need to inform the data subjects about data breaches that could adversely affect them. There is no longer a notification required for the (wholly or partly automatic) processing of personal data. A notification will only be required when there is a breach. This notification must be done quickly, without undue delay. Besides, the organisations will also have to notify the relevant data protection authority.

This means that if the new Regulation enters into force as stated in the proposal, from the day that the Regulation enters into force, the European research projects will no longer need to notify the data protection authority before they start with their experiments (where they process personal data). This is considered to be a major improvement for conducting research in the area of FIRE and IoS in Europe.

4.2. E-Commerce Directive 2000/31/EC

4.2.1. Liability of Intermediaries

EU provisions on liability can be found in a plethora of different legal instruments. One of such instruments is the Directive on e-commerce, which contains specific provisions dealing with the liability of service providers.31

Specifically, this directive refers to the liability of intermediary service providers.32 The main idea behind these provisions can be found in a basic problem created by the Internet. As the Internet can be used as a means to circulate harmful or illegal information it is important to assess who can be held liable for such information. In many cases, however, it will not be an easy task to identify the user that uploaded the information. As a result, such cases are often redirected towards the service provider that hosted the website on which the information was posted or the internet service provider that provides the internet access to the user suspected of uploading the harmful or illegal information. As it may lead to undesirable effects to hold service providers liable for all acts committed by the users of their services, the EU has created a specific framework that governs the liability of these intermediary service providers. The provisions in the directive on liability cover three specific situations and provide a final general provision.

The EU saw such provisions necessary to ensure that no unreasonable burden was put on the intermediary service providers as they play an important role in the development of the Internet and e-commerce, particularly in cross-border transactions. The provisions of the directive relating to these liability issues were therefore almost literally transposed into national law by the

32Articles 12 to 15 Directive 2000/31/EC.
Member States. Although the directive only addressed the three situations discussed earlier, certain Member States have even further expanded this waiver of liability to hyperlinks and search engines.

4.2.1.1. Mere conduit
First, the directive addresses the situation of mere conduit. This means that, when a service provider only transmits the information provided by a recipient of the service, or only provides access to a communication network, this service provider will not be held liable for that transmission. Such is, however, subject to the conditions that the service provider

(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

Even if such information transmission or access provision would include automatic, intermediate and transient storage, such storage would still be regarded as mere conduit if it is conducted for the sole purpose of transmitting information and if the information is not stored for a longer period than necessary for the transmission. Although service providers can under the scope of this provision not be held liable for the nature of the information transmitted, they can be asked to terminate or to prevent an infringement.

4.2.1.2. Caching
A second situation addressed by the directive is that of caching. In the same vein as the provision on mere conduit, service providers are not held liable for the automatic, intermediate and temporary storage of information, if such storage is performed for the sole purpose of making the further transmission of said information to other requesting users more efficient. Also here, this is subject to certain conditions, namely that the service provider

(a) does not modify the information;
(b) complies with conditions on access to the information;
(c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
(d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and

34 Ibid., 13.
35 Article 12 Directive 2000/31/EC.
36 Article 12 (1) Directive 2000/31/EC.
37 Article 12 (2) Directive 2000/31/EC.
38 Article 12 (3) Directive 2000/31/EC.
(e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.\(^{43}\)

As under the previous article, while not held liable, service providers can be asked to terminate or to prevent an infringement.\(^{41}\)

### 4.2.1.3. Hosting

The third specific situation addressed by the directive is hosting.\(^{42}\) If a service provider delivers the service of storing information provided by the recipient of the service, the service provider will not be held liable for the contents of such information. This is, however, subject to the conditions that the service provider

(a) 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) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.\(^{43}\)

Furthermore, the service provider may not control or exercise authority over the recipient of the service and he may still be required to remove the information or block access thereto.\(^{44}\)

The European legislator probably did not foresee the emergence of web 2.0 technology and of new media players taking up the role of new intermediaries. But today we can observe a tendency to broaden the exemption of purely technological players to these new platform operators. Intermediaries such as Facebook, forum keepers, blog services or even bloggers (with regard to comments) providing third parties with a virtual space where they can upload and store their own content have with varying degrees of success made use of the exemption as hosting providers, provided there was no prior moderation, selection of content producers or other active intervention in the content uploaded by the users.\(^{45}\)

### 4.2.1.4. No general obligation to monitor

Lastly, the directive provides that one cannot ask the service providers to monitor all information transmitted or stored by them or to actively locate illegalities therein.\(^{46}\) If service providers are made aware of alleged illegalities concerning the information they transmit or store, they will need to inform the appropriate authorities.\(^{47}\)

\(^{40}\) Article 13 (1) Directive 2000/31/EC.

\(^{41}\) Article 13 (2) Directive 2000/31/EC.

\(^{42}\) Article 14 Directive 2000/31/EC.

\(^{43}\) Article 14 (1) Directive 2000/31/EC.

\(^{44}\) Article 14 (2) and (3) Directive 2000/31/EC.


\(^{46}\) Article 15 (1) Directive 2000/31/EC.

\(^{47}\) Article 15 (2) Directive 2000/31/EC.
4.2.2. Review of the E-Commerce Directive

Approximately a decade after the adoption of the E-commerce Directive, the Commission highlighted that online retail trade still only accounted for less than 2% of total retail trade in Europe. That is why it decided to organize a public consultation “on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC)”.

In the course of the consultation, which ran until the 5th of November 2010, 420 answers were received.

Following these efforts, the Commission published a Communication on “A coherent framework for building trust in the Digital Single Market for e-commerce and online services”. In this Communication, it is stated that in order to boost the digital economy, Member States will have to take action with regard to five priorities:

- First, they should strive to develop the legal and cross-border offer of online products and services.
- Secondly, they should improve operator information and consumer protection.
- Furthermore, they should ensure that payment and delivery systems are reliable and efficient.
- Moreover, Member States should combat abuse and provide for more efficient dispute resolution.
- Finally, they should deploy high-speed networks and advanced technological solutions.

The Commission Communication was accompanied by two Staff Working Documents, one of which concerned “Online services, including e-commerce, in the Single Market”. This Working Document highlighted the need for further clarification on the intermediaries’ regime of the E-commerce Directive. Among other things, this section of the Working Document lamented the unclear scope of the provisions on intermediaries’ liability exemptions. For instance, it is not very clear what the terms “actual knowledge” or “expeditiously” in art. 14 imply. More importantly however, the Working Document also contained an extensive analysis on so-called “notice and action” procedures, which will be further discussed in the next part.

4.2.3. Notice-and-Action Initiative

As described above, art. 14 of the E-Commerce Directive provides for an exemption of liability for hosting service providers: in order to benefit from this exemption of liability, they have to act “expeditiously” to remove or block illegal content when they gain “actual knowledge” of the

---

50 Id., p. 5.
51 Id., p. 8.
52 Id., p. 11.
53 Id., p. 12.
54 Id., p. 15.
56 Id., p. 32-38.
Illegality of said content. The procedures, by way of which these service providers act when removing or blocking illegal content, are the so-called “notice and action” procedures. If illegal content is found on a hosting service provider, one may notify such service provider, following which said provider will then have to act against the illegal content (which may e.g. be racist, contain child pornography or infringe intellectual property rights).

Art. 14(3) of the E-Commerce Directive states the following: “[The liability exemption for hosting] shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal of disabling of access to information.” Hence, this provision allows Member States to lay down rules regulating these procedures in detail. In this regard, The Staff Working Document provides an overview of the self-regulatory and legislative measures taken in the various Member States in this regard.

However, in the Communication discussed above, the Commission noted the need for a uniform European framework on such takedown procedures, because the existence of differences between the laws of the various Member States in this area causes great uncertainty for online businesses. The Staff Working Document, for its part, made it clear that the majority of respondents to the public consultation on e-commerce was in favour of establishing such a European procedure. Moreover, the Working Document went on to define a number of issues that are at the core of the fragmentation and uncertainty in this area. First of all, there is uncertainty regarding the requirements for notice: on the one hand, the notice should be sufficiently detailed for service providers to assess the illegality of the content, but on the other hand, it would be counterproductive to place too heavy a burden on notice providers.

Secondly, there is discussion on the need for enabling “counter-notices” in order to protect fundamental rights such as freedom of expression. The third issue relates to the timeframe for action: there is uncertainty as to when this timeframe starts running, and there is disagreement on the need for clarification of the term “expeditiously”. Fourth, there is the risk of wrongful notices and unjustified takedown of content, and the question of who is to be held liable in such situation (the notice provider or the service provider). Fifthly, it has been argued that it is not desirable to make service providers the (sole) “judges” assessing the illegality of content. And finally, it is highlighted that “notice and action” procedures should complement other policies, like preventive measures.

That is why the Commission decided to launch a public consultation on “procedures for dealing with illegal content on the Internet”, which ran from the 4th of June 2012 until the 11th of

60 SEC(2011) 1641 final, p. 43.
61 SEC(2011) 1641 final, p. 44.
65 SEC(2011) 1641 final, p. 46.
September 2012.\textsuperscript{66} This public consultation was intended to get stakeholders’ views on the transparency, effectiveness, proportionality and fundamental rights compliance of these “notice and action” procedures. In the consultation respondents were asked a number of questions:

- First, respondents were asked about their role and the categories of illegal content they are dealing with.\textsuperscript{67}
- Secondly, respondents were asked to specify whether they felt that takedown is often ineffective or slow, whether takedown of legal content is very common, and whether they felt that there is too much legal fragmentation for hosting service providers.
- Moreover, questions were asked as to the meaning of the term “hosting” and the (lack of) clarity of terms such as “actual knowledge”, “awareness” and “expeditiously”.
- Next, information was sought on existing tools and pages for notifying illegal content, whether these are easy to find/use, and whether hosting providers should have (exclusive) procedures for notification.
- Furthermore, respondents were asked about the modalities of notifications:
  - Should they be done in an electronic format, should they contain contact details, should they allow service providers to identify the alleged illegality easily, should they contain specific details on the illegality?
  - Should there be rules for unjustified notices, and if so, how should such unjustified notices be prevented?
  - Should service providers give feedback to the persons notifying them of an alleged illegality, and if so, how?
  - Should they contact content providers before taking action? Should they first remove or first disable access to the illegal content, or is the sequence irrelevant?
  - How fast should they act? What if law enforcement authorities urge them not to act?
  - How should unjustified action (against legal content) be addressed?
  - Should service providers be liable for that or not? Is there a role for the EU in this, and if so, what kind of regulation should the EU enact?
  - And finally, would different categories of illegal content require different policies with regard to notice and action procedures?

There was a big number of responses but it is difficult to predict when we will be able to learn more about the outcome. The results of the survey have not been officially published, and only a limited number of responses were made public by their suppliers. However, from those public responses it can be deduced that in general, business federations and civil society groups are dealing with a wide variety of illegal content (illegal offer of goods and services, content infringing intellectual property rights, child abuse content, terrorism related content, privacy infringement, etc.). Moreover, a wide category of activities is considered to fall within the scope of the term “hosting”. In addition, there is general agreement on the fact that hosting service

\textsuperscript{66} See \url{http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm} (last consulted on 14/04/2013).

\textsuperscript{67} The Questionnaire, entitled “A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries”, was formerly available at \url{http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=noticeandaction}. 

© Copyright ICRI-KU Leuven and other members of the EXPERIMEDIA consortium 2013
providers should have a procedure in place to notify the presence of illegal content. Furthermore, both civil society groups and business federations seem to agree on the need for rules to avoid unjustified notifications, as well as the need for sanctions in case of unjustified notices. Finally, there is agreement on the fact that there is a role to play for the EU in the field of notice and action procedures. Hence, it seems unavoidable that the EU takes up the issue of notice and action procedures in future revisions of the E-commerce directive.

4.2.4. Consequences of the reforms in the area of liability of intermediaries for FIRE and similar developments

It seems that the main consequence of the review of the E-commerce Directive for FIRE would be a great improvement of legal certainty in the area of liability of internet intermediaries. At the current state of legislation it is not always entirely clear whether certain services qualify for one of the liability exemptions contained in the Directive. It is particularly difficult in case of services, which intend to rely on the exemption for hosting service providers. A vast European case law on this topic proves that courts differ in their opinions on qualification of the new types of services. In Future Internet, where developers constantly come up with new, innovative ways of using third parties’ content such level of legal uncertainty is problematic. It could be even seen as hindering to innovation and development as the providers of new types of applications cannot be sure that they will not be held liable for illegal content provided by their users.

Moreover, the approach presented by the European Commission in their attempt to revise the existing rules shows that they are considered to be inefficient. The revised rules that would clarify the obligations of service providers, with regard to illegal or harmful content of third parties would certainly improve that situation. Such would be the consequence of clear procedures on notice-and-action that would ensure prompt and balanced reaction to illegal content. In addition, it would greatly improve legal certainty for developers of Future Internet services in Europe. Such type of procedure, unified at the EU level would also improve harmonization of the applicable rules between the member states. Currently, the rules regulating this issue are very fragmented throughout different EU countries. It results in difficulties for European research projects with partners from different countries, in applying the correct national legislation on this matter. Such confusion would be inevitably avoided as a result of the more structured and harmonized approach in the revised E-Commerce Directive.

---

4.3. AudioVisual Media Services Directive

4.3.1. Green Paper on AudioVisual Media Services


The TWF Directive only covered “television broadcasting”, i.e. the initial transmission of television programmes intended for reception by the public, that is, an indeterminate number of potential television viewers, to whom the same images are transmitted simultaneously. These are the so-called “linear” audiovisual services. The 2007 AVMS Directive significantly expanded the scope of content regulation to include also on-demand or “non-linear” services. However, the AVMS Directive still makes a distinction between these two categories, not only for definitional reasons, but also in terms of applicable rules: only minimum rules apply to the on-demand services, while an additional tier of stricter rules applies to the linear services. This system is called ‘graduated regulation’ or a ‘two-tiered approach’.

In July 2011, the European Commission published a Green Paper “on the online distribution of audiovisual works in the European Union”, the purpose of which was to assess the effects of technological development on distribution of and access to audiovisual content, with a view to establishing a “digital single market”. In this document, it is highlighted how new technologies have given rise to unprecedented problems in the field of licensing/rights clearance and related remuneration issues. Much of these problems are the effect of the cross-border nature of audiovisual content distribution and access, which has become ever more prevalent since the enacting of the AVMS Directive.

First of all, a lot of content is increasingly being made available on an on-demand basis after the initial broadcast. Furthermore, such content is often also transmitted through the internet or made available for downloading. According to the Green Paper, online transmission not only requires clearance of different rights (like the reproduction right and the right to make available...
compared to traditional broadcasting, it also implicates additional territories, hence necessitating rights clearance for these territories as well.\(^{73}\)

Secondly, as far as retransmission of an initial broadcaster signal by e.g. a cable operator is concerned, it is important to note that this separate copyright act is governed by a different directive, namely the Satellite and Cable Directive.\(^{74}\) This instrument installed a twin-track copyright clearing process: on the one hand, broadcasters may individually license their own (broadcasting) rights and the rights transferred to them by contract to cable operators. On the other hand, all other rights cable operators may need for retransmission should be cleared through collective licensing, i.e. via collecting societies.\(^{75}\) Not only does this twin-track licensing system lead to a lack of clarity and certainty, but in addition it may not be adapted to new technological developments like simulcasting (i.e. simultaneous retransmission via the internet). Whereas the AVMS Directive is founded upon the principle of technological neutrality, the EC Green Paper states that there is discussion on the need to update the technology-specific provisions of the Satellite and Cable Directive to include these technological developments.\(^{76}\)

Thirdly, similar problems arise with respect to transactional video-on-demand services for audiovisual works, which are increasingly being made available simultaneously with theatrical or DVD releases. Here, too, lack of certainty may hinder rights clearance practices, and there are problems with cross-border licensing, since distribution and marketing might be fragmented across different territories.\(^{77}\) Furthermore, in the Green Paper the Commission highlights its commitment to create a framework for online licensing of multi-territorial and pan-European audiovisual services. Special attention should be devoted to the regulation of collective licensing, to ensure better governance and more transparency for collecting societies. Possible strategies include the introduction of a “one stop shop” system for licensing (which would mean that you would only have to address the producer of an audiovisual work), or the application of the country of origin-principle (a principle put forward in the Satellite and Cable Directive) to online programming in general.\(^{78}\) The country of origin denotes the country where the transmission originates, although further research is needed to determine if and how this criterion can be applied to the online environment.\(^{79}\) A third strategy would consist in the development of a unitary European Copyright Code, including a unitary licensing system. And in the meantime, the necessity of updating the exceptions and limitations of the Information Society Directive should be evaluated.\(^{80}\)

Moreover, the Green Paper also laments the lack of uniform rules regarding authorship of audiovisual works as well as regarding the transfer and assignment of rights. Online exploitation would imply that the author or performing artist would have to transfer his “right to make

\(^{73}\) COM(2011) 427 final, p. 8.
\(^{75}\) Arts. 9.1 and 10 of the Satellite and Cable Directive.
\(^{76}\) COM(2011) 427 final, p. 9.
\(^{77}\) COM(2011) 427 final, p. 10.
\(^{78}\) COM(2011) 427 final, p. 12.
available”, but this leads to inequitable remuneration for said persons. That is why the Commission proposes to introduce an unwaivable right to remuneration for authors and performing artists that have made their audiovisual works available on the internet. However, the Commission specifies that this approach might be detrimental to the objective of establishing a Digital Single Market, so other solutions should be explored as well.

Finally, the Green Paper also addresses film heritage institutions, which usually do not own the works they archive, but still want to be able to digitize them, make them available online and screen them in a digital format. They, too, suffer from the lack of clarity and certainty regarding rights clearance, and the Commission recalls initiatives that explore the harmonization of certain copyright exceptions in this regard.

4.3.2. Green Paper on convergence

Recently, the European Commission has adopted a Green Paper on convergence in the media landscape: Green Paper on “Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values”. The document deals with convergence of media services, understood as “the progressive merger of traditional broadcast and internet services”, and the way they are consumed. It is stated that these evolutions require private actors to come up with innovative business models, whereas policy makers should reflect on the need for a public policy response. In this regard, the AVMS Directive, as well as the electronic communications framework, may need to be updated.

For instance, the objective of establishing a Single Market for content is thwarted by language barriers and legal fragmentation in the field of copyright law. Given the fact that the Green Paper on “the online distribution of audiovisual works in the European Union” (discussed above) already addresses copyright issues, the Green Paper on convergence limits itself to calling for the reducing of language barriers. In addition, it is highlighted that US companies don’t struggle with these barriers as much as the domestic EU companies do, and the Commission calls for clarification on the factors explaining this.

One of the most important examples of convergence is that between linear and non-linear media services, the distinction between which is increasingly blurring in Europe and elsewhere. Hence, the “two-tiered approach” of the AVMS Directive (see above) risks creating market distortions which may need to be addressed by policy makers. More specifically, the dual regulation of commercial communications is liable to create disadvantages for European media companies compared to non-EU providers of non-linear services.

Moreover, convergence also has influence on media freedom and media pluralism, and so it must be assessed to what extent new rules are needed to ensure pluralism in a landscape of converged media. Finally, rules on children’s access to content are at risk of becoming less effective due to convergence, so regulatory action might be needed here as well.

81 COM(2011) 427 final, p. 16.
82 COM(2011) 427 final, p. 18.
4.3.3. Consequences of the reforms in the area of media law for FIRE and similar developments

The term “Internet of Services” denotes an evolution whereby software (applications) is increasingly being made available on the internet as a service. Applications are stored on servers and you can consume these services without installing any software on your computer (in this regard, the term is closely related to the term “cloud computing”). Moreover, developers who want to create new applications can use the resources available on the internet and build on existing services, so they don’t have to start from scratch. This allows for better, faster and smoother innovation in the area of services.

Certain elements of the proposed revisions discussed above will prove to be particularly relevant in the light of these evolutions. The creation of new online media services (like YouTube applications, or entirely new services) might be subject to different, stricter rules in the future. First, the Green Paper on the online distribution of audiovisual works in the European Union forebodes a possible future harmonization of copyright laws. The growth of online content distribution calls for clearer and easier rules on licensing (e.g. the application of the “country of origin” criterion, a “one stop shop” system or even the implementation of a unitary EU copyright code).

Secondly, the Green Paper on “Preparing for a Fully Converged Audiovisual World” announces possible changes in the way the European legislation deals with non-linear services. The two-tiered approach (a different legal regime for linear and non-linear services) is at risk of creating market distortions, so this approach may need to be lessened. This will most likely result in the enacting of stricter rules for non-linear services. Such changes will definitely have an impact on online media services, given the fact that these online business models will usually be categorized as non-linear services.

Whereas harmonization of licensing regimes will most likely prove to be beneficial to online services distributing audiovisual content, stricter rules for non-linear services will not be welcomed by online media services. In sum, the proposed reforms will provide new opportunities and at the same time create new challenges for media services on the internet.
5. Terms and Conditions for API developers

5.1. Introduction

Another issue that is extremely relevant for research projects in FIRE is compliance with the Terms & Conditions of the underlying platforms. In case of the EXPERIMEDIA project, this refers mainly to Social Networking Sites. As was described in the earlier deliverables some of the experiments plan to develop applications that would use the critical mass of the existing popular SNS like Facebook or Twitter. In the Driving Experiments of EXPERIMEDIA this was the case with the Experiment at Schladming, while a possible SNS application at FHW was planned only for the later stage of the project. In the 1st Open Call Experiments some of the experiments at Schladming and FHW consisted of building applications for Facebook (MEDIAConnect, BLUE, REENACT). This could also be the case in the 2nd Open Call experiments. For this reason the issue of compliance with the SNS’s Terms & Conditions is addressed in this deliverable.

The Internet of Services allows building applications on top of an existing platforms or software. This is possible by virtue of the application programming interface (hereinafter “API”) provided by these platforms. An API, described very simply, is ‘a set of programming instructions and standards for accessing a Web-based software application or Web tool’\(^{84}\). Developers interested in creating such applications for SNS are required to use the API of the targeted software specified by its provider. Moreover, providers of the targeted SNS platforms specify rules on leveraging content from the underlying SNS – so called developers’ Terms & Conditions (hereinafter “T&C”) or Terms and Conditions for API. What follows is that the applications developed in the framework of EXPERIMEDIA project must be, on one hand, interoperable with these platforms, and on the other, compliant with their T&C’s. As will be shown below, such compliance with the Social Networks’ T&C by the developers of application can influence the final shape of the application and therefore is a relevant issue that must be addressed accordingly.

T&C’s, in general, are addressed to anyone interacting with the Social Network platform that includes traditional users of the SNS as well as programmers or developers of applications. However, different T&C’s exist for these two groups. The rules for traditional users, who provide content to SNS, are less stringent than those for developers, who also extract content through the platform’s APIs. In this section we will focus solely on the T&C’s for the application developers, since it is this type of document that is important for EXPERIMEDIA developers.

The presented analysis is focused on the T&C’s of the most popular SNS like Facebook and Twitter. However, it is possible that in the 2nd Open Call experimenters will focus also on other SNS. It is not possible to conduct a detailed analysis of all the existing platforms, especially without specific information about the intended application. For this reason, the presented analysis might require updating at the further stage of the project.

\(^{84}\) http://money.howstuffworks.com/business-communications/how-to-leverage-an-api-for-conferencing1.htm
5.2. Relevance of the API T&C’s

T&C’s of SNS provide a list of conditions under which the developers building applications on top of the underlying SNS, are allowed to access and exploit such content. As described by Twitter, these documents ‘describe the policies and philosophy around what type of innovation is permitted with the content and information shared on’ a particular SNS. For this reason, they are sometimes called ‘a letter of law of the platform’.

First of all, it should be clarified that T&C’s are considered to be a legal agreement between the SNS provider and any developer or programmer building an application that would utilize content from this SNS through its APIs. In fact, they are considered to be a contract between the SNS and the application developer. This contract outlines the rights, obligations and limitations of the application developer. It also contains warranties and disclaimers made by the platform provider with regards to the platform.

This contract is entered into by adhesion. This means that the developer does not need to express his consent to the given rules. His consent is implicitly inferred from his use of the platform. Therefore, there is no negotiation process of the conditions, even though T&C’s are considered to be a contractual agreement. This is a specificity of an adhesion contract in which the only party that decides about the contract is the one with greater bargaining power. In case of T&C’s, which govern basically every aspect of the provider-developer relation, the rules are determined by the SNS providers in their complete discretion. This could be described as a ‘take-it-or-leave-it’ situation, as all the power rests on one side of the contract. Disagreement with any of the terms usually results in no license being granted to use the APIs.

Moreover, the developer must ensure that the application he plans to introduce complies with all the described conditions. The SNS usually reserves itself a power to monitor the way the API is used by the developers. If the SNS provider discovers that the developer exceeded, or attempted to exceed, the given limitations, they might block, temporarily or permanently, the developer’s ability to use the SNS’ API and its content.

The provider of the SNS often reserves the right to completely change, or redesign the given rules. Typically no prior notification is deemed necessary, although the recent trend is to announce the upcoming changes publically, for instance through a blog post. As it is openly admitted, SNS try to keep up with the developers and adjust the rules along the way. In its T&C’s Twitter specifies that ‘the Rules will evolve along with our ecosystem as developers continue to innovate and find new, creative ways to use the Twitter API, so please check back periodically to see the most current version’. Facebook is even more straightforward about its ability to implement changes without notice, stating that they ‘can change these Platform Policies at any time without prior notice as we deem necessary. Your continued use of Platform constitutes acceptance of those changes’. The consequence of this could be that a developer

---

85 Twitter Developer Rules of the Road, https://dev.twitter.com/terms/api-terms
86 Facebook Platform Policies: http://developers.facebook.com/policy/
87 Twitter Developer Rules of the Road, https://dev.twitter.com/terms/api-terms
89 Facebook Platform Policies: http://developers.facebook.com/policy/
violates the given rules because he did not check them for a period of time and they have changed dramatically since he first introduced his product.

T&C's provide conditions and requirements regulating how the application developers can interact with and leverage the SNS content. The described rules are rather extensive and provide very detailed specifications. The issues they most commonly regulate refer to extracting content, posting content, communication with the users, their privacy, or transfers of data to third parties, etc. The rules are a combination of technical and legal requirements. Together, they create a full image of the SNS’ philosophy on accessing and exploiting its content.

The terms of legal nature refer mainly to the issues of privacy and data protection, but also intellectual property rights. An example of such term, in Twitter, is: ‘Respect the privacy and sharing settings of Twitter Content. Do not share, or encourage or facilitate the sharing of protected Twitter Content. Promptly change your treatment of Twitter Content (for example, deletions, modifications, and sharing options) as changes are reported through the Twitter API’. Facebook specifies that ‘Subject to certain restrictions, including on transfer, users give you their basic account information when they connect with your application. For all other data obtained through use of the Facebook API, you must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on your application’. Both of these terms should be linked to the provisions of the Data Protection Directive and its principles of data processing.

In the area of intellectual property rights Facebook’s policies provide that ‘In the United States you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a "notice and takedown" process. In other countries, you must comply with local copyright laws and implement an appropriate "notice and takedown" process upon receiving a notice of claimed infringement’. This provision refers to the topic of liability exemptions for the providers of the hosting services. As was described in the previous section of this deliverable, ISPs are required to promptly react to the notification of an infringement through an adoption of the specific “notice and take down” procedures from the applicable national law.

It is, however, strictly technical requirements that predominate the rules in T&C's. An example of such term from Twitter is: ‘End users must be presented with the option to log into Twitter via the OAuth protocol. End users without a Twitter account should be given the opportunity to create a new Twitter account as provided by Twitter. You must display the Connect with Twitter option at least as prominently as the most prominent of any other third party social networking sign-up or sign-in marks and branding appearing on you Service’. Another example would be ‘Your website must offer an explicit "Log Out" option that also logs the user out of Facebook’.

90 Twitter Developer Rules of the Road, https://dev.twitter.com/terms/api-terms
91 Facebook Platform Policies: http://developers.facebook.com/policy/
92 See more in Deliverable D5.1.2 Ethical, legal and regulatory framework for social and networked media.
93 Twitter Developer Rules of the Road, https://dev.twitter.com/terms/api-terms
For the compliance assessment the technical execution of both types of the conditions matters most. It is therefore the comprehension of the terms by technical partners/entities that will have a crucial impact on the level of compliance with T&C’s. In this process, they should be guided by the legal partners/entities to ensure proper understanding of the legal grounds of some of the conditions.

T&C’s specified in so many details by the platform provider have several goals. The main one of course, is to protect the business of the platform provider. It should not be forgotten that a SNS provider is a for-profit company. As such, it has its own business interests that it needs to protect from anyone whose business model might be conflicting with theirs. This could be the case when an application profits too much from the freely accessible content of the SNS and becomes very successful. In such situation there is a risk it could become a direct competitor of the platform. Hence, platform providers introduce rules and limitations for developers to prevent this. The situation is however very dynamic, as new applications are constantly developed and new, creative ways of using SNS content are introduced. This is the main reason why the platform providers continue to adjust the rules and make them stricter. Twitter openly admits, that some of its ‘updates and modifications may adversely affect how your Service accesses or communicates with the Twitter API. If any change is unacceptable to you, your only recourse is to terminate this agreement by ceasing all use of the Twitter API and Twitter Content. Your continued access or use of the Twitter API or any Twitter Content will constitute binding acceptance of the change’95.

Platform providers monitor closely the application ecosystem. They also demand that the developers cooperate with them, especially in case the application requires a large amount of API calls. As stated by Twitter ‘One of the key things we’ve learned over the past few years is that when developers begin to demand an increasingly high volume of API calls, we can guide them toward areas of value for users and their businesses. To that end, and similar to some other companies, we will require you to work with us directly if you believe your application will need more than one million individual user tokens’96. Facebook is more explicit in its requirement that once an application makes a serious impact in the ecosystem, more stringent rules will apply: ‘If you exceed, or plan to exceed, any of the following thresholds please contact us as you may be subject to additional terms: (>5M MAU) or (>100M API calls per day) or (>50M impressions per day)’97.

Next to the main goal of T&C’s it is possible to distinguish a secondary goal, which is the protection of the SNS traditional users. After all it is their content that the application will target. Such protectiveness by the platform contributes to the transparency and fairness towards their users. These users very often are not aware how the applications process their data. By introducing certain limitations SNS platforms actively defend users’ interests, particularly in the area of privacy protection and intellectual property rights. The example of such term would be the requirement for explicit consent by Facebook, as mentioned above. This requirement allows

---

95 Twitter Developer Rules of the Road, https://dev.twitter.com/terms/api-terms
97 Facebook Platform Policies: http://developers.facebook.com/policy/
for more control of the personal data by the users and is in line with the on-going review of the Data Protection Directive, as described in the previous sections of this deliverable. The main incentive of such paternalistic behavior, very often, is an understandable attempt to avoid a possible vicarious liability for the developers’ activities. Nevertheless, the effect that the stringent rules have on the overall protection of the users’ interests should not be disregarded.

5.3. Compliance with the API T&C’s

All the aspects described above prove that compliance with the T&C’s of the platform should be given proper attention, preferably from the very beginning of the application development. This task, which is often ignored, could backfire causing problems for the developer. The developer’s lack of awareness of T&C’s is, however, not the only complication. As will be presented below compliance with these terms can be problematic, for a number of practical reasons.

The main difficulty encountered by the developers is the interpretation of the terms. The rules are not only drafted unilaterally, but they are also subject to the exclusive interpretation of the platform provider. As Facebook states in their T&C’s: ‘We can take enforcement action against you and any or all of your applications if we determine in our sole judgment that you or your application violates Facebook Platform Terms and Policies’\(^98\). This simply means that it is entirely their decision to assess who is playing by their rules and who is not. The platform provider is basically not interested in accepting any interpretation of its rules that would differ from their perspective. Their view, however, is rarely presented to the public in its entirety. Some explanation is usually provided but it seldom is exhaustive enough to clarify all the doubts.

This can be particularly problematic in case of provisions that are phrased in a vague manner. An example of such term could be one from the recent Twitter updates, stating that: ‘No other social or 3rd party actions may be attached to a Tweet’. With no additional explanation on what is meant by a ‘3rd party action’, and whether email clients (“Email link”) and web browsers (“Open in Safari”) would count as such, this wording created a state of panic among the developers.\(^99\)

It is clear that by keeping their cards close to their chest platform providers ensure they have an upper hand in case of any conflict regarding compliance with T&C’s. This is because effectively there is no possibility to contest their opinion. There is a strong chance that all the ambiguities with regard to the understanding of the provisions will be resolved to the disadvantage of the application developer. This could happen even if he attempted to comply with a term, but achieved a result that was not satisfactory to the platform provider. As a consequence ‘Twitter can decide your app is breaking a (potentially vague) rule at any time, or they can add a new rule that your app inadvertently breaks, and revoke your API access at any time’\(^100\).

Another factor complicating bona fide attempts of compliance is the frequency of changes to the T&C’s. As shown above, platform providers reserve themselves a right to rewrite the given

\(^98\) Facebook Platform Policies: http://developers.facebook.com/policy/
\(^99\) Arment M., Interpreting some of Twitter’s API changes, 16 August 2012, http://www.marco.org/2012/08/16/twitter-api-changes
\(^100\) Arment M., Interpreting some of Twitter’s API changes, 16 August 2012, http://www.marco.org/2012/08/16/twitter-api-changes
conditions anytime, and any way, they feel necessary. This means the rules can change from one
day to another, possibly without any warning. Any possible future changes are very difficult to
predict. They reflect the business interest of the platform providers which are the most urgent to
protect. There is, however, no possibility to foresee their nature or the extent of thereof. This is
of course within their prerogative as the platform owner. Nevertheless, it creates a grave
difficulty for the developers who can never rest assured that their application continues to
comply with all the requirements. This makes T&C’s very unstable and unpredictable; offering
no guarantee as to whether something will be permitted in the future.\textsuperscript{101} This makes the existence
of the applications very precarious.

The only option the developers are left with is a continuous re-assessment of their application
every time an update is announced. In case of a problem, the choice is between re-designing the
application or its certain functionalities or dropping it completely. As a result, the compliance
control is a never ending process from which the developer can never retire if he wants his
application to continue existing. This means, ‘that anyone who builds a product on a third- party
platform, especially a free one, risks losing everything, anytime, on a moment’s notice’.\textsuperscript{102}

5.4. Preliminary conclusion

All these aspects of compliance with T&C’s are equally relevant for EXPERIMEDIA but also
other research projects. It is crucial to highlight that there are no exceptions created for research
activities, which would make the situation of a research project any easier. As can be imagined,
the continuous changes and re- assessments can lead to serious delays of the project. The only
solution that the research projects are left with is to pay constant attention to T&C’s of the
targeted platforms and react promptly to their changes. If such need occurs, they can also
contact the targeted platform provider and enquire about special conditions for scientific
purposes. There is however no guarantee that such exception will be granted.

Within the EXPERIMEDIA project, specific analysis is conducted by experimenters for
different experiments, depending on the need. The conducted analysis is focused on the goals,
objectives and functionalities of specific experiments. This means that the correct approach for
one of them might not necessarily be correct for another. It is also done only for the SNS that
these experiments target. A tailored approach is therefore required.

It should be underlined that it is not an intention of the EXPERIMEDIA project to provide
legal advice on interpretation of legal documents in the type of T&C’s. The goal of the presented
considerations is to raise the awareness to the importance of this issue to the project partners, as
well as other EU research projects. It seems that until now, this aspect of research and
development was often neglected. Such approach, however, could have serious implications,
both technical and legal, for the consortium as a whole and its specific partners. In

\textsuperscript{101} Arment M., Interpreting some of Twitter’s API changes, 16 August 2012,
http://www.marco.org/2012/08/16/twitter-api-changes
\textsuperscript{102}Phelps A., Twitter’s API changes will have a real impact on news developers, Nieman Journalism Lab, 17 August
2012, http://www.niemanlab.org/2012/08/twitter-api-changes-will-have-a-real-impact-on-news-developers/?utm_source=Weekly+Lab+email+list&utm_campaign=650bc81e79-
WEEKLY_EMAIL&utm_medium=email
EXPERIMEDIA, due to its specific character, a constant attention is paid to the compliance issue. This means that with the presented analysis might require an update, if such need occurs, when the 2nd Open Call experiments are selected.
6. Conclusion

All of the legal considerations presented above have been taken into account by the partners in the EXPERIMEDIA project.

The presented deliverable addressed three regulatory areas that are most important for the EXPERIMEDIA project: privacy and data protection, liability of intermediaries and media law. The developments that were described in this deliverable include the proposal of the new Data Protection Regulation, the initiative on notice-and-action, and the Green Paper on the online distribution of audiovisual works in the European Union, as well as the Green Paper on convergence (Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values) that has currently been adopted. All these developments show that the European Commission is aware of the main problematic issues for the Future Internet is preparing regulatory response to tackle them. However, the works are still far from completion. This means that extensive analysis of the consequences of these developments is difficult to conduct. It seems also that majority of them will not really affect the experiments in EXPERIMEDIA. The effects of the Data Protection review, which is the most advanced one, can hardly be expected before 2015. The same applies to the discussions in the area of Media Law. Nevertheless, close attention is paid on the on-going discussions to prepare the project partners for the changes that are coming up.

Compliance with T&C’s of the underlying Social Networks is another issue very relevant for the EXPERIMEDIA project. The terms are often very restrictive and at the same time can be very vague which makes their interpretation cumbersome. Moreover, they change frequently, possibly without any notification. The main conclusion is that the relevance of T&C’s should not be disregarded because it could greatly affect the whole project. However, no uniform answers can be provided as each experimenter should always perform their own analysis and interpretation of the T&C’s having in mind their goals, objectives and functionalities they want to offer. Partners in EXPERIMEDIA are aware of the compliance issues that could affect their applications. Depending on the type of experiments selected in the 2nd Open Call, an update to provided analysis might be required at a further stage of the project. The results of the research conducted on the compliance with SNS T&C’s will be also fed into the activities of the European Competence Centre. This Competence Centre will be established by the end of the project (Task 5.2.4) to gather, organise and exploit knowledge created by the project, as well as other previous projects, and use it to advance Future Internet Research and Experimentation into social and networked media systems.