

## Extended Executive Summary of SPICE Deliverable D1.6

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
<b>2</b>	<b>Privacy &amp; Data Protection.....</b>	<b>3</b>
2.1	General.....	3
2.2	Profiles.....	4
2.2.1	Privacy Risks of Profiling.....	4
2.2.2	Evaluation of Data Processing for Profiles.....	5
2.2.3	Design Proposals .....	5
2.3	Location Based Services.....	6
2.4	Data Transfer.....	7
2.4.1	Data Transfers crossing national state borders.....	7
2.4.2	Data Transfers into Countries without an adequate level of data protection	8
2.4.3	Conclusions.....	8
<b>3</b>	<b>Intellectual Property Rights .....</b>	<b>9</b>
3.1	The copyright issues in SPICE: general .....	10
3.2	Copy right law in SPICE.....	11
3.2.1	DRM and watermarking.....	11
3.2.2	Technical modifications.....	14
3.2.3	User Generated Content.....	14
<b>4</b>	<b>Commercial communication .....</b>	<b>15</b>
<b>5</b>	<b>Proposed Improvements for European Law .....</b>	<b>16</b>
5.1	Privacy and Data Protection.....	16
5.1.1	Profiles .....	16
5.1.2	Location Based Services .....	17
5.1.3	Data Transfers.....	17
5.2	Intellectual Property Rights.....	18
5.2.1	General Recommendations on copyrights .....	18
5.2.2	Digital Rights Management and watermarking.....	20
5.2.3	Technological modifications.....	21
5.2.4	User Generated Content.....	21
5.3	Marketing and Advertising.....	21

## 1 Introduction

SPICE (Service Platform for Innovative Communication Environment) is a Framework Program 6 research project that aims at the design of an innovative technological infrastructure for the creation and delivery of ICT services (hereinafter “service platform”). The service platform will support the creation, deployment and delivery of various services in the information society. The service platform will also be used to deploy and commercialise new communication services or to distribute (enriched) content. Such a technological infrastructure raises a number of legal questions. Three legal aspects seem to be particularly relevant for the functioning of the SPICE service platform. These three aspects are:

- Privacy and data protection law;
- Copyright law;

- The regulation on (unsolicited) commercial communication

These legal fields and their relevance for the service platform were in depth researched and described in SPICE Deliverable 1.6<sup>1</sup>. Herein only a summary and the main findings of such research are presented. For more detailed explanation the reader is advised to look into Deliverable 1.6.

The importance of **privacy and data protection** for the service platform is a double one: not only should it be a matter of compliance to laws and regulation by developing products respecting legal and regulatory requirements, but privacy concerns are also a matter of trust and respecting interest of the service platform's future customers. There are three major issues within data protection and the functioning of the service platform: **Profiles, Location Based Services and Data Transfer**.

Regarding the **copyright law**, the services that are deployed within the service platform often involve the creation, the publication and the delivery of 'content' to the platform's end-user. The content that is handled by the service platform more often than not consist of material that is protected by copyright and/or other rights related to copyright. Therefore the first crucial issue is to understand when 'content' is protected by exclusive rights, and what exclusive rights and exceptions are relevant in the contexts of the electronic delivery of 'content'. Additionally, the following issues have been identified as particularly relevant for operation on the service platform: **Digital Rights Management and watermarking, technological modifications, User Generated Content (UGC)**.

For the third legal aspect described, i.e. the **commercial communication**, the main supposition is that the service platform will primarily assist commercial service providers in seeking new business opportunities and business models. Without a doubt, the issue of the commercial communication and the revenue stream it produces are relevant factors in taking business decisions. When discussing commercial communication the main questions are the legality of commercial communications: an opt-in system for unsolicited communications, possible sanctions for spamming, and methods of handling unsolicited communication by intermediaries.

The conducted research focussed on the European legal framework, which has been analysed and applied to the service platform. The relevant legal aspects discussed are mostly regulated by European directives. A directive imposes the Member States to achieve the objectives set out in the directive, but leaves the possibility to the Member States to choose the most appropriate means to achieve these goals. Consequently, the harmonisation of national laws by means of directives remains limited (differences in the national applicable rules continue to exist), and in a particular case, the national legal rules implementing European directives still need to be consulted.

---

<sup>1</sup> Anna Moscibroda, Christoph Schnabel et al., SPICE Deliverable 1.6, Legal Issues and Regulation, May 2008, [http://www.ist-spice.org/documents/SPICE\\_D1.6\\_FINAL\\_CC.pdf](http://www.ist-spice.org/documents/SPICE_D1.6_FINAL_CC.pdf)

## 2 Privacy & Data Protection<sup>2</sup>

### 2.1 General

There are three directives on data protection enacted by the European Community: The general Data Protection Directive<sup>3</sup> the E-Privacy Directive<sup>4</sup> and the Data Retention Directive.<sup>5</sup>

The Data Protection Directive is applicable only to the processing of personal data. Article 2 (a) of the Directive defines personal data as “any information relating to an identified or identifiable natural person”, called data subject. Thus, whether data is personal data or not depends on the circumstances and the context it appears in. The directive does not differentiate between different kinds of data, with the exception of “sensitive data” being addressed later. There is no data that is too trivial to not fall under the directive. Data that is rendered anonymously is not relating to an identifiable natural person. Also excluded from the protection are any data referring to legal entities/persons. The E-Privacy Directive is not restricted to natural persons but also protects the fundamental rights and freedoms of legal persons. It does not apply to activities concerning public and state security, defence and state activities in the area of criminal law. In these areas the Data Retention Directive makes use of the exception stipulated in art. 15 of the E-Privacy Directive, which allows to restrict the rights and obligation provided for in that directive, *inter alia* for reason of detection and prosecution of criminal offences. The E-Privacy Directive in art. 5 obliges the providers of publicly available communication networks to guarantee the confidentiality of communication. This applies as well to the content of communication as to any data accumulated during the communication.

After the transposition of Data Retention Directive, Internet service providers (ISP) and telecommunication operators will be obliged to store the communication data of all their users and subscribers for a period of 6 to 24 months. “Data” means traffic and location data and the related data necessary to identify the subscriber or user according to art. 1 (2) of Data Retention Directive. Any data referring to the content of the communication is excluded from the ambit of the directive. The data is destined for the investigation, detection and prosecution of serious crime. The Data Retention Directive is heavily disputed for political and legal reasons. Ireland has filed an action before the ECJ to annul the Directive 2006/24/EC because of a lack of competence of the legislating bodies

---

<sup>2</sup> For the distinction between privacy and data protection we refer you to introduction of D1.6.

<sup>3</sup> Directive 95/46/EC of the European Parliament and of the Council 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, OJ L 281, 23.11.1995 pp. 31 – 50, (hereinafter Data Protection Directive).

<sup>4</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 pp. 37 – 47, (hereinafter E-Privacy Directive).

<sup>5</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54 – 63, (hereinafter Data Retention Directive).

namely the European Parliament and the Council.<sup>6</sup> But until this case is decided the Data Retention Directive remains valid and applicable law. Some European countries have already started with its transposition.

## **2.2 Profiles**

Personal profiles can pose a bigger risk to an individual's privacy than most other data collections. Profiles are by definition more than just a large collection of personal data. Within a profile data will be linked purposefully to gather additional information going beyond what can be learned from the original data<sup>7</sup>. This additional information is based on conclusions drawn from the linking of the data.

### **2.2.1 Privacy Risks of Profiling**

There are two basic problems: through the combination and linking of seemingly harmless information new and maybe even sensitive data can be generated that could reveal insights into financial or health problems of the individual. If this happens, the data processor may know information about the individual which he/she never gave away. Problems can arise also through a loss of context. When the additional information is separated from the basic information it was derived from, the conclusions cannot be verified. Thus the loss of context can lead to a distorting shortening of the original information and thereby compromise the reliability of the information gathered within the profile altogether. In particular, a change of behaviour that led to the conclusion of the additional information may not necessarily lead to the change of the additional information itself. To get the data processor to change the additional information about oneself may pose much more difficulty than changing the original information. The individual could thus lose control over the image others have of him/her, while-in principle- it must remain in the hands of the individual to define his/her appearance within his/her social context.

The most important thing to be learned from the technical basics<sup>8</sup> is that one has to differentiate three different categories of data. The first category of data is the preferences that the end-user him/herself submitted to the system. The second category is the user-history. This includes the whole history of usage of services of the service platform. The user-history is needed, amongst other things, to analyse the behaviour of the end-user to conclude preferences of the end-user other than the ones he/she submitted to the system him/herself. These preferences of the end-user are not learned from him/her, but through the Association Rule-Based Learner and belong to the third category of data.

The three categories differ in several ways, but the most important difference is the level of control the end-user has about them. An end-user can decide for him/herself which kind of information he wants to enter as preferences into his/her profile and how detailed he/she wants it to be. An end-user could even enter inaccurate data, if he/she does not want certain information about him to be known by the service platform. This would

---

<sup>6</sup> Action brought on 6 July 2006 in case C-301/06, OJ C 237, 30.09.2006, p. 5, accessible via <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:237:0005:01:EN:HTML>

<sup>7</sup> Scholz, P., *Datenschutz beim Internet-Einkauf*, Baden-Baden 2003, p. 95

<sup>8</sup> Inquiry into technical basis of profiling was based on the SPICE Deliverable 4.1, *Ontology Definition of User Profiles, Knowledge Information and Services*, December 2006.

influence the performance of the profile negatively, but it is an effective way of protecting one's privacy. The level of control decreases as far as the user-history is concerned. This information will be stored for profile use without any confirmation being necessary by the end-user. The only way he/she has influence on the user-history is by changing behaviour or by completely turning the service off and simply live at least temporarily without the advantages the service platform has to offer. The end-user has the least control over the additional information that is gathered by evaluating the user-history with the help of the Association Rule-Based Learner. This is completely uncontrollable by him/her, since he/she has no influence on the algorithms and the conclusions that are drawn from his behaviour.

### **2.2.2 Evaluation of Data Processing for Profiles**

The Data Protection Directive stipulates grounds on which the data processing is legitimised (art.7). A contract between the SPICE operator and end-users could, because of the provision of art. 7 (b) of the Data Protection Directive, legitimise the data processing that is necessary for the service platform to deliver the envisioned features for end-users. But there are certain conditions implied. The contract should contain a separate part that explicitly and extensively explains the data processing that is necessary so that end-users can assess the risk for their privacy they take when deciding to sign a contract with a service platform operator. It is thus necessary for the service platform operator to provide the future customers in the contract with information they can comprehend and thereby assess the situation correctly. It can be said that future customers must be informed about the three different categories of data that were explained above. Only then can the provision of art. 7 (b) of the Data Protection Directive be fulfilled.

The Data Protection Directive distinguishes only one special category of personal data: sensitive data. Such data is defined by art. 8 para 1 of the Data Protection Directive as any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. Profiles created for the service platform will inevitably contain sensitive information, because every set of data that directly or indirectly indicates information as listed in art. 8 para 1 of the Data Protection Directive shall be considered sensitive<sup>9</sup>. Article 7 (b) of the Data Protection Directive can only legitimise the processing of non-sensitive data. So the question arises what provision this processing could be based on. Article 8 para 2 (a) of the Data Protection Directive states that the processing of sensitive data shall not be prohibited, when the data subject has given his explicit consent to the data processing. SPICE could in these cases base the processing on the consent given by the data subject.

### **2.2.3 Design Proposals**

1. Sensitive data should be separated from "normal" data and be stored under heightened data security safeguards. It is of utmost importance that these data may never be accessible by accident without authorisation.

---

<sup>9</sup> Dammann, U., and S. Simitis, *Die EG-Datenschutzrichtlinie – Kommentar*, Baden-Baden 1997, art 8, margin 7.

2. The end-user should at all times be in full control of his/her profile, and especially the preferences listed in his/her profile. This means that the end-user must be able to access the profile at any time and be able to delete any part of the profile he/she does not want anybody (including the service platform operator) to know about without any chance of the profile data being restored.
3. The same holds true for the user history. The end-user must be able to control his/her personal user-history. It does not matter whether the information stored in the user-history is correct or not, whether the end-user has or has not used the services listed. There must be a possibility for end-users to delete all or certain parts of the user-history at any time and thus decide for themselves whether they want the service platform to “remember” this.
4. There should be a possibility to turn off the association based rule-learning. End-users should be able to decide which of their activities and decisions made by them should be the basis for the rules and preferences stored in their profile. This is not only a matter of data protection, but could also help to improve the accuracy of the data. If a SPICE end-user does already know that the decision he is about to make will be an exception to his/her usual behaviour it makes sense for him/her to be able to switch off the association based rule-learning.
5. End-users must also be in control over the rules that were developed with the help of the Association Based Rule-Learner. Though the rule may in fact describe the behaviour of the end-user correctly and thus may be helpful in predicting the choices to be made by the end-user, it must still at all times be up to the end-user to decide which of this information should be stored in his personal profile and which should not.

### **2.3 Location Based Services**

The legal framework for processing location data is very complex. To determine which legal provisions apply when service providers or private parties are processing personal, location and traffic data is nothing short of a “Herculean task”<sup>10</sup>. It is also questionable whether the European framework is able to protect user privacy adequately due to the unclear definitions and unresolved legal questions. Though the current legal situation may call for criticism, it is still applicable law and it is the only law on a European level dealing with these questions. We will not go into the details of these problems here, but rather refer to the extensive dealing with these issues in SPICE Deliverable 1.6.

The best solution for SPICE again seems to be to put the user in the centre of attention and give him the possibility to decide who has access to his data and who has not. Of course a balance between usability and fine-grained consent management will have to be found. Users should neither have to consent into data processing every few minutes nor be reminded only every other month that they are being localised constantly. In the end it all boils down to a matter of trust.

These are the design proposals we have worked out:

1. Users must be able to object to the localisation at any time, by simple means and free of charge. This is more than a mere proposal, but a direct requirement of art. 9 para 1 and 2 of the E-Privacy Directive.

---

<sup>10</sup> Roosendaal, A., B.-J. Koops and C. Cuijpers (eds.), *The legal framework for location-based services in Europe*, FIDIS (Future of Identity in the Information Society) Deliverable D11.512, June 2007, via <http://www.fidis.net/resources/deliverables/mobility-and-identity/#c1791>, p. 10.

2. Users should not be tracked on an ongoing basis, but only when requesting a Location Based Service. Thus the users do not have to object to localisation, when not requiring it, but can instead avoid being localised by simply not using a Location Based Service.
3. In those cases where the very nature of the Location Based Service requires an ongoing localisation (like emergency services or childwatch) users have to be reminded on a regular basis about their possibility to turn off the localisation service.
4. Mobile devices that allow the users themselves to simply turn off localisation are preferable to those solutions where the user has to ask the operator to stop tracking him. This way the user does not have to trust the operator but stays in control of his location data him/herself.
5. Where the providing of a Location Based Service necessarily calls for the involvement of other parties, the user's identity should not be disclosed to them whenever it is possible to avoid it. This includes the service platform operator having to conduct the payment to the other actors.

## **2.4 Data Transfer**

The operation of a service platform may require the transfer of personal data from one data controller to another. When this happens, it is indeed processing of personal data – in particular ‘disclosure by transmission’ – to which data-protection law applies. Transfers from a data controller to one or more other controllers may for instance be transfers of personal data (telephone number, location data, traffic data, emails...) from a telecommunication provider to a location-based service provider. Transfers may also consist of forwarding personal data (like messages) from a (intranet) platform to a web publisher who publishes or automatically allows for publishing the personal data on an Internet website. In these examples, data-protection law applies, thus also the grounds for legitimising the data processing (in this case data transfer) need to be respected. Two main grounds are the consent of the data subject for the processing of the data, and the contract to which the data subject is the party, and fulfilment of which requires data processing (art. 7, paras a). and b).). This is true for every disclosure by transmission, be it inside one country or crossing national borders from one country to another. Following we will deal with data transfers across national state borders in particular.

### **2.4.1 Data Transfers crossing national state borders**

Following the provisions of Data Protection Directive<sup>11</sup> there is a distinction to be made between data transfers of personal data within the European Community and the European Economic Area and transfers of personal data to other countries. Transfers of personal data within the European Community and the European Economic Area are not different from data transfers within a country. In addition to all those members of the European Community and the European Economic Area the Commission has also decided that some more countries provide an adequate level of data protection although they are not a member of either the European Community or the European Economic Area (like Argentina, Switzerland and so on). Transfers of personal data into those countries are possible. However, particular problems arise in case of transfer of data to countries that do not provide for an adequate level of data protection.

---

<sup>11</sup> Articles 25 and 26 of the Data Protection Directive.

## **2.4.2 Data Transfers into Countries without an adequate level of data protection**

There are still ways to legitimise a transfer into a country not providing for an adequate level of data protection:

- The Safe-harbor-Agreement
- Standard Contractual Clauses
- Binding Corporate Rules

These three ways are providing for safeguards when there are no adequate data protection safeguards demanded by law in the respective the data recipient is located in. For a thorough examination of these possibilities we refer to the respective sections in SPICE Deliverable 1.6.

Another possibility to legitimise a data transfer into a country without an adequate level of data protection is granted under art. 26 para 1 of the Data Protection Directive. This article allows for said data transfers when, *inter alia*, they are based on unambiguous consent of the data subject or when the transfer is necessary for the performance of a contract between the data subject and undertaking wishing to transfer the data. It is obvious that these provisions make it substantially easier to transfer personal data into a third country where no effective data protection can be guaranteed for.

Despite the fact the derogations listed in art. 26 para 1 of the Data Protection Directive may allow for transfers into third countries without an adequate level of data protection without further safeguards like binding corporate rules or standard contractual clauses (as foreseen in art. 26 para 2), they do not provide an exemption from the rule that fundamental rights must be respected<sup>12</sup>. To ensure this, national data protection authorities can intervene at any time and demand that an international transfer of personal data should be carried out on the basis of such additional adequate safeguards as foreseen by art. 26 para 2 of the Data Protection Directive, and thus precluding possibility to rely on the derogations in para 1, if this is necessary to prevent the possibility of a breach of the data subjects' fundamental rights.

## **2.4.3 Conclusions**

The platform operator should always limit data transfers to the scope absolutely necessary; only relevant, adequate and non-excessive data can be processed. End-users should be informed when signing the contract that data transfers to other actors may become necessary, the categories of data to be transmitted and who the possible recipients of his/her personal data are. When data transmissions become necessary that are not covered by the contract, the service platform operator must get the individual, unambiguous and informed consent of the data subject to legitimise the transmission.

For sensitive data different rules apply. The transmission of personal, sensitive data poses the highest risk for the privacy right of the data subject and his right not to be subject to discrimination. The processing of such data is therefore principally prohibited. If the transfer of personal, sensitive data should be unavoidable (for instance a picture or a

---

<sup>12</sup> Article 29 Data Protection Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, November 2005, via [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf), p. 9

'sensitive' location needed for a service), it can nonetheless not be legitimised by being necessary for the performance of a contract, since that is, according to Art 8 para 2 Directive 95/46/EC not a legitimation for the processing of sensitive data. Thus, in case any sensitive data are transmitted, the data controller must seek for the prior informed and explicit (written) consent of all data subjects involved (which is higher standard than unambiguous and informed consent which applies in other cases).

### 3 Intellectual Property Rights

The SPICE platform aims at facilitating the distribution of the digital services. Those services, in principle, consist of offering the digital 'content' to the platform's users. The content that is handled by the service platform could consist of raw data, facts, etc., but also of photos, videos, music, multimedia files, etc. It is fair to assume that the content that will be handled by SPICE will to a large extent consist of material that is protected by copyright and/or other rights related to copyright.

The copyright law determines, *inter alia*, how to distinguish between legally protected and unprotected content, which exclusive rights are granted and to whom, what are the limitations to those rights. Those legal rules are in detail presented in SPICE Deliverable 1.6, and thus only the main principles are presented below. Such general rules will be followed by comments on a few topics of particular importance for SPICE: Digital right management and watermarking, technological modification and User Generated Content.

The legal framework on copyright is complex. The regulation takes place at the international, European and national level. As the harmonisation at the international and European level is not complete, the national law regulates a number of aspects of the copyright regime, and remains central in determining legal relations. Despite the fact that harmonisation on the European level is not complete, the European regulation of copyright and related rights remains the common denominator of the copyright regulations of all the Member States, and therefore it constitutes the basis for the legal assessment of the service platform and its operation.<sup>13</sup>

---

<sup>13</sup> Such framework consists of the following legal acts: EEC Directive of 14 May 1991 on the legal protection of computer programs, OJ L 122, 17.05.1991 *PP*. 42 - 46 (Amended by Council Directive 93/98 EEC of 29 October 1993). (further referred to as Computer Program Directive) Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ L 345, 27.22.1992, pp. 61-66 (further referred to as Rental Directive); Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and related rights of copyright applicable to satellite broadcasting and cable retransmission, OJ L 248, 6.10.1993, pp. 15-21 (further referred to as Satellite and Cable Directive); The Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, OJ L 290, 24.11.1993, pp. 9-13, as amended in 2001); Directive 06/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases OJ L 77, 27.3.1996, pp. 20-28 (further referred to as Database Directive); Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L 320, 28.11.1998, pp. 54-57; Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24, 27.1.1987, pp. 36-40. Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art, OJ L 272, 13.10.2001, pp. 32-3.

### 3.1 *The copyright issues in SPICE: general*

Copyright does not protect ideas, factual data or languages. It protects the formal expression of original “works of art and literature”<sup>14</sup>, a very broad and open concept, that even includes computer programs and databases. Copyright protection is granted to original works, no other criteria are applied. Thus, the copyright protection does not depend on the quality, novelty, or professional skill of the author. It is important to remember that not only professional content is protected, but user generated content (UGC) can enjoy copyright protection too. Additionally, the rights related to copyrights grant the exclusive right to the performers (such as singers, musicians, actors and dancers), producers of phonogram, film and database producers and of broadcasting organisations. Though often a certain investment is required for a related right to arise, the amateurs are not precluded from being regarded as performers or producers.

Copyright grants a number of **rights** to copyright holders, both moral and economic rights. These rights are exclusive rights, meaning the right-holder has a right to authorise and to prohibit certain uses of protected works (i.e. protected content).

With regard to the service platform, two moral rights are particularly relevant: the right to be recognised as the author (or performer) of a work (the ‘paternity’-right), and the right to oppose any modification of the work (or performance) that might be prejudicial to the honour or reputation of the author (or performer) (the ‘integrity’-right).<sup>15</sup> The service platform certainly threatens the existence and enforcement of the moral rights: protected content is easily communicated to the public without mentioning the authors (and performers) or cut, mixed, adapted or otherwise modified in disregard of the right of integrity.

The economic rights which are relevant for the service platform are: the exclusive right of reproduction (including adaptation) and the exclusive right of communication to the public, including the right of making available to the public.

The **reproduction right** might become relevant in connection with a number of actions undertaken by the service platform, e.g. when content is uploaded to the repository, a permanent reproduction is made. The process of technologically protecting the content also implies reproductions and often even modifications. Reproductions are also made during the process of delivering the content to the end-users. All those reproductions are covered by the author’s exclusive reproduction right.

The service platform offers content to the end-users by broadcast or on demand (e.g. by streaming or downloading). Depending on how the services operate, the acts can be qualified as a **communication to the public** and, as the case may be, more specifically, as a **making available to the public**, which specifically refers to digital online interactive forms of distribution.

In order to undertake actions that fall within the scope of any of those rights, the service platform needs to obtain **authorisation** from the right holders, unless the conditions of an exception are fulfilled. If the intended use is not (or not entirely) covered by any

---

<sup>14</sup> The Berne Convention on the protection of literary and artistic works, signed in September 1886, (<http://www.wipo.int/treaties/en/ip/berne/>), Article 2.

<sup>15</sup> Those right are harmonised only on the international level, Notably by the Berne Convention, art 6bis in respect of the moral rights of authors, and the WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on December 20, 1996; <http://www.wipo.int/treaties/en/ip/wppt/>, art. 5 in respect of the moral rights of performers.

exception, then a licence needs to be negotiated with all right holders, including the authors and the performers as holders of the moral rights.

The process of obtaining licences can be very burdensome. Due to the territoriality of the copyright, a service provider needs to obtain **a licence for each particular territory (country)** on which he wishes to provide his services. Inversely, no service involving protected content can be offered on a territory that is not covered by the licence. Consequently the availability of the content may depend on the geographical location of the SPICE user. Moreover, different persons may hold rights in the same content and these different owners may not be identifiable as such at first glance, which adds to the complexity of contracting.

### **3.2 Copy right law in SPICE**

The copyright law principles are difficult to translate into the design principles. The copyright and rights related to copyright prohibit exploitation of the protected subject matters without the prior authorisation of the rights holders, except in some narrow cases covered by exceptions. Two further conclusions can be derived for that requirement: First, authorisation (a licence) needs to be sought in order to legally use the ‘content’, unless exceptions can be invoked. On the other hand, a legitimate use (e.g. allowed under exception) should not be prevented. Second, basically any use of ‘content’ is allowed if it falls within the scope of right-holder’s authorisation. In other words, copyright does not pose an absolute restriction on usage of works (thus also to the SPICE plans on using the ‘content’), and it does not define other mandatory requirements than to engage into negotiations to obtain the licences and respect exceptions, if applicable.

However, certain SPICE specific recommendations can be made in the following areas: Digital Rights Management (DRM), technological modifications, user generated content (UGC).

#### **3.2.1 DRM and watermarking**

European law addresses technological measures by means of three directives: the Computer Program Directive,<sup>16</sup> the Conditional Access Directive<sup>17</sup>, and the Information Society Directive.<sup>18</sup> The provisions in respect of the technical protection measures in the Information Society Directive are the most comprehensive, have the broadest scope, and are also the most relevant for the service platform.<sup>19</sup>

---

<sup>16</sup> Council Directive 91/250 EEC of 14 May 1991 on the legal protection of computer programs OJ L 122 , 17.05.1991, p. 42 - 46 (amended by Council Directive 93/98 EEC of 29 October 1993), (hereinafter Computer Programme Directive).

<sup>17</sup> Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L 320, 28.11.1998, pp. 54–57, (hereinafter Conditional Access Directive).

<sup>18</sup> European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–9, (hereinafter Information Society Directive).

<sup>19</sup> The protection provided under the Information Society Directive does not apply to the technical protection of computer programs, which are subject to the Computer Programme Directive. The provisions of other directives relating to the technical protection measures (including those of Computer Program

The Information Society Directive does not refer to DRM systems or watermarking as such. Instead, it provides protection of technological measures (art. 6) and of rights management information (art. 7), which are generally part of more complex DRM-systems or constitute the basis of watermarking services. The directive protects such technology against circumvention and tries to re-balance it with the copyright exceptions.

The Information Society Directive provisions on the protection of technological measures consist of two main blocks. First, the Directive prohibits actual acts of circumvention (art. 6 (1)). Secondly, the Directive prohibits dealing in circumvention technology (art. 6(2)). The rights-management information is protected against removal or manipulation (art. 7 (1)(a)), but also the dealing in copies from which such information has been removed can be prohibited (art. 7(1)(b)).

As far as the circumvention provisions are concerned, the most important aspect for the technology developers is the question what technology qualifies for legal protection.<sup>20</sup> The technical measures should meet the criteria defined in the Directive in order to qualify for protection. Those criteria can be summarized as follows:

- the legal protection relates to ‘technology’, ‘devices’ and ‘components’, thus it encompasses software and hardware, digital and analogue technology.<sup>21</sup>
- the measures need to be ‘designed to prevent or restrict’ acts which are not authorized by the person holding the rights of the content.
- the technological measures must prove to be “effective” in order to enjoy protection.<sup>22</sup>

The criterion of effectiveness is the most unclear and problematic.<sup>23</sup> It can be understood as granting the legal protection only to those technological measures which ensure actual protection: obsolete devices or Technical Protection Measures (TPMs) which are too easy to circumvent enjoy no protection.<sup>24</sup>

Then, the question is which rights-management information is legally protected. Rights Management Information is the information that identifies the protected content, its author or other right holders or the terms and conditions of use. The protection

---

Directive) have been presented in the Deliverable 1.6, *European legal framework on copyright*, section 2.3.4.2.3, and therefore are not elaborated in this contribution.

<sup>20</sup> For description of other issues relating to technological prevention of circumvention (e.g. the scope of the protection of technical measures) we refer to the SPICE Deliverable 1.6.

<sup>21</sup> Bechtold, S., in: Dreier, T., Hugenholtz, P., (eds.), *Concise European Copyright Law*, Kluwer Law International, The Netherlands, 2006, p. 386.

<sup>22</sup> Art. 6(1) of the Information Society Directive.

<sup>23</sup> Art. 6 (3), second paragraph of Information Society Directive offers a presumption of what constitutes an “effective” technological measure: a measure “*shall be deemed effective, where the use of a protected work or other subject matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject matter or a copy control mechanism, which achieves the protection objective.*” Criterion of effectiveness, however, remains unclear. More in Spice Deliverable 1.6.

<sup>24</sup> Institute for Information Law (IVIR), University of Amsterdam, *Study on the implementation and effect in Member States' laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Part 1: Study on the implementation and Effect in Member States' Laws of Directive 2001/29/Ec on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*, Final Report, The Netherlands, February 2007, p. 168. [http://ec.europa.eu/internal\\_market/copyright/docs/studies/infosoc-study\\_en.pdf](http://ec.europa.eu/internal_market/copyright/docs/studies/infosoc-study_en.pdf), p. 75.

encompasses the digital representation of this information, e.g. a number. Not only is the information protected, if it is attached to or included in the physical carrier of the protected content, but also when it 'appears' in connection with a communication to the public. Only electronic rights-management information is protected, whether it is visible to the user or hidden. Legal scholars explicitly mention watermarks and metadata as falling under this definition.<sup>25</sup>

Another issue is 'fingerprint' information. A fingerprint does not aim at providing information on the author, right owner or use restrictions. It aims at embodying information on the purchase operation and/or purchaser into the file. Thus, a fingerprint is not rights-management information, according to the definition of the Information Society Directive. Moreover, due to privacy considerations, information identifying the consumers is explicitly excluded from this protection (recital 57 of the Directive). As the fingerprinting raises concerns under the privacy law, it is advised to consider this technology with consciousness.<sup>26</sup>

Another aspect is the relation of the technological protection measures to the copyright exceptions. Since the technological protections may hamper some specific legitimate use of the protected content, the European legislation provides some means to restore the balance between the (absolute) technological protection measures and the interests of the beneficiaries of exceptions. The Information Society Directive requires Member States to impose obligations to respect certain copyright exceptions, despite technology applied to protect the content (however, the directive allows a right holder to override the application of these exceptions in case of a contract for all online interactive forms of providing services, i.e. those available on demand). Such obligation concerns the exceptions that are adopted by particular Member States, and the States are free to choose which of the exceptions allowed under the directive they wish to adopt.<sup>27</sup> The Member States are also free to choose the way of reconciling the technological restrictions and usage of content allowed by exceptions.<sup>28</sup> Such freedom limits the harmonisation effect of the Directive.

Despite the fact such obligation is not directly addressed to a technology provider or intermediaries (e.g. SPICE), the technology provider, on behalf of the right holder, could be required, or even forced, to lift the TPMs. In that respect the architecture of content protection and delivery should be flexible enough to allow access despite the terms of use initially encoded, and to provide the possibility to allow a user to reproduce the content. Thus, SPICE should clarify with the right holders in which circumstances the TPMs should yield to the respect of the exception.

The issue of content protection technology is not only addressed by copyright law, but some crucial issues are also tackled by consumer protection and privacy laws. As regard

---

<sup>25</sup> Bechtold, S., in: Dreier, T., Hugenholtz, P., (eds.), *Concise European Copyright Law*, The Netherlands, 2006op. cit., p. 394.

<sup>26</sup> It needs to be remembered that when a fingerprint contains personal data on the purchaser of the content, his/her consent for fingerprinting is required

<sup>27</sup> Article 5 states only one exception is mandatory and needs to be implemented in all Member States (so called 'temporary copy exception'), and provide for the long list of facultative exceptions which may, but do not have to be adopted by Member States.

<sup>28</sup> The Directive basically only prescribes which form the allowed exception are eligible for such strengthen legal protection (Information Society Directive, art. 6 para 4 ), however the choice to implement exceptions remains with Member States.

the later, data protection and privacy law applies to DRMs and watermarking each time personal data are involved (e.g. for profiling purposes).<sup>29</sup>

DRM systems may violate consumer rights, by restricting the lawful use of the purchased product. This is when the consumer protection can come into play. In respect of the consumer protection law several design recommendations aiming to ensure the transparency and fairness of DRM systems should be taken into consideration. Those are:

- Informing consumers on technology used, its main characteristics, i.e. in which way it limits using the content;
- Transparency also requires easy interfaces, clear information regarding the condition of services offered and access to additional info (full information on services and their conditions, including the charges and the legal conditions of the licences);
- Support for a variety of different business models that could actually improve the choice for the consumer;
- Technological protections must not hamper normal processing of content.

### **3.2.2 Technical modifications**

The service platform imposes several **modifications to the content**, during the compression and encoding in the DRM scheme, during the reformatting of the multimedia files, changing the content modality or resolution. The question rises whether such modifications constitute the acts restricted under the copyright regime.

Without a doubt, the exclusive right to reproduction comes to play in case of the technical modification of content. In some jurisdiction also the specific adaptation right could be invoked in such cases. As the adaptation right is not, in principle,<sup>30</sup> harmonised, the national legal systems define whether and when it can be invoked, and where the border line between the reproduction and the adaptation rights runs. On the other hand, it is doubtful whether SPICE could rely on any exception to copyright to undertake such modification without authorisation of the right holders. Furthermore, technological modification may also prejudice the moral right of integrity. Therefore, the proper authorisation(s) of all right holders should be sought to undertake such modifications. Ultimately, the national laws of the Member States determine whether the required license should cover the right of reproduction, the right of translation or adaptation, or both, and the moral rights. National law will also determine the rights of the service platform as the adaptor of the content.

### **3.2.3 User Generated Content**

The service platform gives the end-user the possibility of interacting with the content and enriching it. The user can tag the content, annotate, write reviews, or otherwise modify the content, and create and upload new content.

The law on copyright and related rights applies equally to user generated content. That means the user-creator, while enriching the content, might be using someone-else's

---

<sup>29</sup> The recommendation re privacy has been presented in Section 2 *Privacy and Data Protection* above.

<sup>30</sup> European law harmonises the adaptation right only in cases of software and databases, see art. 4 of the Computer Program Directive and art. 5 of the Database Directive.

legally protected content. In case such use of content falls within the protection of an exclusive right and no exception is applicable, the user needs to obtain the authorisation of all the right-holders concerned. Such an obligation only concerns the person who is actually reusing the content, and does not necessarily pose an obligation directly on SPICE, although end-users should not be encouraged to interact with the content disseminated by SPICE when such interactions are not allowed by right holders.

The application of the copyrights law and law on related rights to the UGC also means the user-creator can become an author or holder of a related right. In other words, the content he produces (e.g. a picture, his record of the song) might qualify for legal protection by copyright or related rights, and the user-creator might then be holder of, both moral and economic rights. The rights of user-creators should be respected equally to the rights of professional content providers. Thus, the user-creator's authorisation should be sought to use his content. On the other hand, the service platform operator should enable the user who wishes to publish his content via SPICE to be recognised as author of the content he produced (with real identity or pseudonym, if they wish), and to express the usage policies he/she wishes to apply to the creations (e.g. in a way similar to Creative Commons<sup>31</sup> licences, though additionally 'all right reserved' option should also be provided). In that respect the watermarking service can provide a useful tool, on the condition it provides the information visible to other users.

## 4 Commercial communication

As the service platform aims at supporting commercial activities, the relevant issues are also those relating to the general legal rules on commercial communication. In that respect the main question is the legality of commercial communications. European law does not regulate the issue of commercial communication comprehensively, thus national rules need to be consulted. However, the European Legislation foresees an opt-in system for unsolicited commercial communications. Therefore, as the general rule, the advertisers need to obtain the consent of the individuals for advertising. As far as the marketing practices pose a threat to privacy, they are subject to the privacy laws when the processing of personal data is at stake (i.e. profiling for the purposes of marketing, which will most likely be done by SPICE).

The service platform will most often be an intermediary, delivering the commercial communication, and collecting consent for the marketing practices and collection of data. Moreover, the service platform might need to deploy technical measures against spam. In doing so it should apply the following guidelines:

- Messages marked as spam and thus blocked should *not* immediately be deleted. End-users should have the possibility to reconsider the automated decision by the spam filter.
- End users should have influence on the spam filter and decide which commercial messages are spam to them and which are not.
- End users should be able to opt-out of the use of the spam filter altogether. There should also be an easy way of opting back into the scanning of e-mails to avoid spam.
- Users should be informed on measures adopted.

---

<sup>31</sup> <http://creativecommons.org/>

## **5 Proposed Improvements for European Law**

In this section we will recapitulate the results of the researched issues with regards to the efforts the European legislation should take to improve the situation.

### **5.1 Privacy and Data Protection**

At the moment the focus of data protection legislation on a European level as well as in the legislation of the Member States is on public safety and security issues. Discussions about data retention, passenger name records to be transferred into the USA and video surveillance dominate the public, political and scientific debate. In such a situation it is especially difficult to raise interest in topics that are important for a private processing of personal data.

However, as we have seen in the course of this deliverable there are some unresolved issues in the field of data protection that deserve attention. Some laws and provisions are outdated, others have never been up-to-date. Some provisions are formulated unclear which makes their applicability hard to determine, for other fields no regulation exists at all. In some cases the regulation takes an overly lax approach, in others the key principles cannot be upheld anymore due to substantial changes in the practised processing of personal data. We will discuss the proposed changes in the order of the researched issues: Profiles, Location Based Services and Data Transfers.

#### **5.1.1 Profiles**

Although profiling techniques have been thoroughly researched from a technical as well as from an economic point of view, still no explicit regulation of these issues exists, neither on a European nor on a national legislation levels. The little case law that exists on the matter, and the legal doctrine deal nearly exclusively with compulsory profiling that is done in the fields of criminal investigation (for dragnet searches for example) or in market research without the data subject knowing that such profiles exist on him/her. But nowadays profiles are used to a large extent in the very interest of the data subject. The end-users of SPICE's services provide the service with preferences and user-history themselves. They do it to enjoy the benefits of the profile in form of a higher level of usability.

The European legislator must face these changes in the development and use of profiling techniques and provide for an adequate regulation of profiling techniques. It should allow for using such techniques to provide personalised services and to support data subjects in organising their daily lives. The regulation must on the other hand guarantee that data subjects will at any point be in control of their profiles. It must be avoided that decisions on behalf of the data subject are made, that the data subject can neither control nor change. Also the data subject must be aware that profiles about him/her exist, what they contain and what they are used for. The current situation in which profile processing is evaluated on basic regulation not made to match the specific risks and advantages of profiling is unsatisfying.

### **5.1.2 Location Based Services**

Since Location Based Services were expected to become a killer application and provide for large business volumes, the European legislator has dealt with these services and provided for regulation on location data in E-Privacy Directive, which all Member States had to transpose into national law.

However, the legal framework for Location Based Services is far from being perfect. There is a huge amount of unresolved issues like the relation between personal data, traffic data and location data. The legal definitions, e.g. definitions of “publicly available electronic communications service” and “electronic communications network” in some cases provide more questions than answers. The technical possibilities to locate users and make use of that location data are developing rapidly and are overtaking the regulations. Some of the answers given by the legal framework are not satisfying and impracticable like asking for user consent at every instant. If Location Based Services are being used heavily, the constant asking for user-consent will become an annoyance to the end-user. The chances are high that end-users may give consent without considering and the giving consent will be reduced to a mere technicality without any significance to the end-user and thus lose its status as an efficient safeguard against privacy intrusions. Also the constellation of offering Location Based Services in a Three-Party-Structure (involving a location provider like a mobile operator), the additional privacy problems it may bring as well as the privacy enhancing effects that can be generated with it, do not seem to have been considered in the process of developing the provisions on location data.

It cannot be said whether the lack of commercial success of Location Based Services is because of a lack of legal certainty or whether the legal issues have not been resolved, because of a lack of case law, due to the fact that Location Based Services have not been used at a large scale. However, to decide about the applicable legal framework cannot be left to the free market. The (European and national) legislator must provide for a clear, understandable and adequate legal framework with sufficient safeguards to meet the risks Location Based Services may pose the privacy of its users. Although he has tried to do so in E-Privacy Directive it cannot be denied that he failed at least in providing a clear and understandable framework. A revision of the legal framework for Location Based Services based on the few experiences gathered so far seems necessary.

### **5.1.3 Data Transfers**

The transfer of personal data across national state borders has, in contrast to the two subjects discussed above, been approached with great attention. The first directive ever to be enacted in the field of data protection already included detailed provisions on the transfer of personal data (cf. Art. 25, 26 of Data Protection Directive).

In the beginning data protection was often considered to be an obstacle to the free developments of the markets and thus the Data Protection Directive is not only on data protection, but also “on the free movement of such data”. Although it is a legitimate goal not to restrict data transfers more than necessary, the transfer of personal data into a country that provides no adequate level of data protection poses a severe risk for the data subject’s privacy. Once the data have been transferred to another country there is no way to guarantee any safeguards, stop unfair processing or even know what is happening with

the data. If the data comes to a country that is notorious for the misuse of personal data and violations of privacy, the data subject may be without any protection at all.

Because of this the transfer of personal data deserves special attention. The European legislator has paid special attention to these problems, but unfortunately “solved” the problems by providing for a number of ways to allow for data transfers into countries without an adequate level of data protection.

The Data Protection Directive provides data exporters with three other possibilities to legitimise data transfers: The Safe-harbor-agreement, standard contractual clauses and binding corporate rules. These are all possibilities to transfer data into a country where the legal framework may not guarantee any protection at all. To top it all off Art 26 para 1 Directive 95/46/EC allows for data transfers, when the data subject has given his consent, the transfer is necessary for the performance of a contract or even when the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.

These provisions allow for a wide range of possibilities to transfer personal data into countries like for example Nigeria, which is notorious for its misuse of personal data. The Art 29 Working Party has paid great attention to these questions and issued a number of working papers and opinions and has called for a responsible use of these provisions, but this cannot be a substitution for a working and consistent legal framework.

The European legislator has to revise the provisions on the transfer of personal data. The result must be a system that is easy to understand, with a limited number of exceptions that all guarantee the same level of protection for the data subject and demand the same level of effort from the data controllers. At the moment it is hard to imagine that any company would rather develop binding corporate rules on a multinational level than to simply gather consent from the data subject.

The fact that data transfers are nearly impossible to track or even be noticed by the data subject is making enforcement of a regulation that should be followed by data controllers hard enough. The situation should not be complicated further by a system of inconsistent rules and problematic exceptions.

## **5.2 Intellectual Property Rights**

### **5.2.1 General Recommendations on copyrights**

Despite the several directives which attempt to harmonise various aspects of copyright within the European Union, it is still fairly difficult for businesses to distribute protected digital content Europe-wide. The first reason is the territoriality of copyrights, meaning that the exclusive rights granted by state law are confined to the borders of this state. The territoriality has its consequences for the licensing of copyright. In order to legally exploit a protected content, the licence needs to be obtained for each work, each right concerned, and each state territory. The process of clearing the right might be quite burdensome. The European Commission is aware of that problem and decided to address the issue in the Recommendation on the collective cross-border management of copyright and related rights for legitimate online music services,<sup>32</sup> which encourages the granting of multi-

---

<sup>32</sup> Commission Recommendation of 18 May 2005 on the collective cross-border management of the copyright and related right for legitimate on-line music services (2005/737/EC), OJ L 276/54, 21.10.1005.

territorial licences on music for online use. The issue is also mentioned in the recent Communication on Creative Content on-Line in the Single Market.<sup>33</sup> The Communication identifies the problem of clearing rights and a multi-territorial licensing as a challenge in developing the digital content industry. It remains to be seen whether any further European legislative action will be taken to address those problems. However, from the point of view of the service providers it is crucial to closely monitor any developments, and if appropriate solutions do not emerge, there is the need to consider simplifying the licensing by means of the binding legal act.

The second factor that might cause difficulties for actors who would like to use the SPICE infrastructure to operate Europe-wide is the limited harmonizing effect of the European copyright law. The issue to solve in that respect is the scope of the rights granted, and their potential overlap, e.g. between the rights to reproduction and communication to the public. Also, it could often be problematic to distinguish between 'communication to the public' and 'making available to the public', especially in case of highly personalized services. The legislator should consider clarifying the scope of the exclusive right (especially the reproduction right) and borders between those rights to avoid the double payment for the same acts of exploitation.<sup>34</sup> In that respect account should be taken of the recommendations already expressed in the doctrine, e.g. by pointing out the possibility of purpose oriented definitions of the exclusive right of reproduction.<sup>35</sup>

Furthermore, most exceptions foreseen in the European Directives are facultative exceptions. Member States may adopt them if they wish, but they are not obliged to do so. It is highly recommended to remedy this lack of harmonization.

While the undertakings could still be expected to have enough resources and knowledge to deal with the complexity of copyright regulation, the same is not true for end-users. The problem especially gets its prominence in the mobile scenario, where people use services while they cross national state borders. The end-users should not be expected to realise the complexity of copyright in cross border contexts. The end-user should not be prevented from using the service only because he/she changes location, or face the liability for acts which are legal in his country and are outside the scope of exception applicable in another country (the users relying on the private copy exceptions in their own country, for the same acts of exploitation of content could face sanctions in another). The request for simplification and greater harmonization of copyright has already been advocated for in the doctrine as prerequisite for the successful development of the on-line services in Europe.<sup>36</sup> The mobile scenario emphasises the difficulty in providing the content-based services. In order to develop such services there is a need for a harmonization of copyright, or even a need for a 'European copyright'.

---

<sup>33</sup> Communication for the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of Regions on Creative Content Online in the Internal Market (Com(2007) 836 final, Brussels, 3.01.2008).

<sup>34</sup> More detailed recommendation relating to those matter can be found in SPICE Deliverable 1.6.

<sup>35</sup> Institute for Information Law (IVIR), University of Amsterdam, *Study, op. cit.*, p. 168.

<sup>36</sup> See especially: Institute for Information Law (IVIR), University of Amsterdam, *Stud, op. cit.*

### **5.2.2 Digital Rights Management and watermarking**

Digital rights management and rights management information remain the important elements in the digital distribution of the protected content. The law provides, on the one hand, for the protection of those technologies against removal and circumvention (and/or trading in circumventing technology), and on the other hand tries to balance the technology with the legitimate use of the content by the beneficiaries of the copyright exception. In both respects we can observe some shortcomings of the European legal framework.

As far as the legal protection of the technological measures is concerned, it seems the law protects a wide range of technologies that aim at enforcing usage restrictions. The problems which arise are the definition of protected measures (i.e. what the requirement of effectiveness means), and the determination of the precise scope of protection. The rights management information is also protected under the Information Society Directive. The scope of protection is broad enough to encompass the watermarking techniques. While using the watermarking might be, in many respects, beneficial (e.g. it might facilitate commercial exploitation of the UGC, and the data on author and right holder would be easier accessible), serious concerns are raised by the fingerprinting technology. It is recommended that the policy makers devote attention to this technology in order to devise adequate safeguards for users, in case it is broadly adopted. It could be considered to protect 'fingerprinting' data as a category of non-personal data protected under the privacy law.

However, more crucial is the relationship between the technological protection and the copyright exceptions. Current provisions of the Information Society Directive that aim at defining the balance between the technological restrictions of usage and the exceptions are very complicated, often unclear. Those provisions hardly provide any harmonisation; first as it is up to the Member States to adopt the exceptions, then it is up to the Member States to define a way the exceptions adopted in that particulate states will be reconciled with technical protection measures in practice. This lack of harmonisation and clarity of the legal rules makes the compliance with such provisions a challenge. Furthermore, in the contexts of the innovative personalised services the practical effects of these provisions can be made obsolete, as the law allows the right holders to disregard the copyright exceptions when the technological protection measures are used in relation to the on-demand services. The ambiguity of the legal provision relating to the balancing technology and copyright exceptions can occur particularly problematic for the technology providers and intermediaries, like SPICE. While there is no direct obligation imposed on those undertakings, in practice it is often the task of the technology provider who carries the burden of adjusting the technology to the request of the beneficiaries of exceptions. Hence, it is highly recommended to revise and simplify the provisions of Information Society Directive relating to balancing the rights of beneficiaries of exceptions. It is especially recommended to reconsider the role, obligations and the liability of the technology providers and intermediaries in that respect. There is a need to provide them with much clearer rules which could be taken into account when designing their business models and the technology as such.

### **5.2.3 Technological modifications**

Undertaking purely technological modification of the content is often necessary in order to offer value added personalised services. It is clear that such modifications of the content fall within the scope of the exclusive reproduction right and thus should be covered by a licence. The technical modifications are, however, often only the intermediary stages in delivering the content to the end-user. In order to deliver the content electronically, one needs to obtain the licence allowing doing so. As the interests of the right holders are safeguarded with a licence in any case, one could reconsider the phrasing and scope of the ‘temporary copy’ exception, as to include the purely technical modifications within its scope.

### **5.2.4 User Generated Content**

In principle, the general copyright framework, including its main principles, apply to the User Generated Content (UGC). However, new technologies make it much easier to interact with existing content, create new content, and disseminate its results to a wider public. The user-creator can thus be a user of the content created by someone else, and then the issue of infringing other’s rights emerge. The user-creator can also become an author or the holder of a related right. Then, the crucial issue is the management of the right he acquires upon creation.

As regards the first point, it is crucial to provide a comprehensive, clear information campaign informing the user-creator on the principles of copyright, the rights they need to respect, and the rights they acquire themselves. The European Union could encourage Member States to undertake such information campaigns in order to promote the creativity amongst the EU citizens.

The second issue raises the need to reconsider the way the UGC content is managed. Currently, several means exist for the user to express their usage policy, e.g. the Creative Commons license. The watermarking technique is also promising in that sense. Further attention should be devoted to monitoring and facilitating means for users ensuring their rights are expressed and respected.

## **5.3 Marketing and Advertising**

The European framework on Spam is not fully comprehensive, but it does provide for general rules on unsolicited advertising. The main problem, however, remains enforcement. Currently, sanctions for spamming are foreseen by national laws only, while spammers operate worldwide. It could be desirable to consider facilitating the actions against spammers worldwide, if not by penalising at the European level, then by facilitating actions against spammers. The current revision of the E-Privacy Directive<sup>37</sup> reaffirms in explicit terms the right of ISPs to initiate the court action, and grants such

---

<sup>37</sup> Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, COM(2007) 698 final, Brussels, 13.11.2007

possibility to the consumer associations and trade unions. Voices also rise in favour of group actions by citizens.<sup>38</sup>

---

<sup>38</sup> European Data Protection Supervisor, *Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10\\_e-privacy\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf).