D3.8

Copyright and Portrait Rights in Digital Persona on Online Social Networks

v 0.8 / 2016-02-08

Niels van Dijk, Katja de Vries and Mireille Hildebrandt (iCIS-RU)

Building on D3.3 this document presents an analysis of the copyrights involved in content and digital persona on OSNs. It also investigates to what extent (an analogue to) the portrait right could provide users of OSNs with an effective legal remedy to restrict the exercise of IP rights by OSNs, notably with regard to IP rights in the profiles compiled or constructed based on user generated content and behavioral data of OSN users. The report concludes with some design implications for the DataBait tool, which will be a included in the legal coordination and integration (T3.6) during the remainder of the USEMP project.

Project acronym	USEMP
Full title	User Empowerment for Enhanced Online Presence Management
Grant agreement number	611596
Funding scheme	Specific Targeted Research Project (STREP)
Work program topic	Objective ICT-2013.1.7 Future Internet Research Experimentation
Project start date	2013-10-01
Project Duration	36 months

Work package	WP3
Deliverable lead org.	ICIS
Deliverable type	Report
Authors	Niels van Dijk, Katja de Vries, Sari Depreeuw and Mireille Hildebrandt (iCIS)
Reviewers	Rob Heyman (iMinds) Adrian Popescu (CEA)
Version	0.6
Status	Xxxxx
Dissemination level	PU: Public
Due date	2015-12-31
Delivery date	2016-04-04

Version	**Changes**
0.1	Initial Release, Niels van Dijk and Katja de Vries (iCIS)

0.2	Review Rob Heyman (iMinds)
0.3	Mireille Hildebrandt (iCIS)
0.4	Niels van Dijk and Katja de Vries (iCIS)
0.5	Adrian Popescu (CEA)
0.6	Niels van Dijk (iCIS)
0.7	Sari Depreeuw (iCIS)
0.8	Niels van Dijk and Katja de Vries (iCIS)

Table of Contents

1. Introduction

In this deliverable we present an analysis of the rights involved in the user profiles on Online Social Networks (OSNs). Apart from data protection, in this way we want to explore what other legal avenues of empowerment a user might have with regard to her data on OSNs. Here we focus no longer only on individual data, but also on the more broad digital personae that are made of users on and by OSNs. This legal analysis will be two-folded. First, we will analyze whether copyright can empower the user with regard to profile which is compiled or constructed based on her user generated content and behavioral data and, most likely, those of other OSN users. Here we will turn especially to database rights on user profiles. Second, we will explore whether image or portrait rights could provide the user of OSNs with an effective legal remedy to restrict the exercise of intellectual rights by OSNs, especially the intellectual rights on her user profile that an OSN might hold.

In order to understand the function of this deliverable, we have to situate it against previous and parallel legal research strands performed within the USEMP project. The three strands of legal research are (a) “Fundamental Rights Protection by Design for OSNs”; (b) “Profile transparency, trade secrets and Intellectual Property rights (IPRs) in OSNs”; and (c) “Copyrights and portrait rights in content posted on OSNs”. These sets of rights described in these three research strands relate to each other as cards in game of user empowerment and disempowerment. It is a fluent and complex ‘game’ in which one right might trump another but none of the rights can be designated in advance to be the ultimate trump – it all depends on the particular circumstances and rights involved which player will ‘trump’ the others. Deliverables 3.1 and 3.6 explored the empowerment of end users with regard to their data through data protection law, mainly by dealing with issues of profile transparency. In the present deliverable we will explore additional legal tools for user empowerment with regard to their data through intellectual rights and image rights. In deliverables 3.2 and 3.7 the focus shifted to the relation between profile and profiler by looking into the rights on the side of OSNs and third parties. It explored their intellectual rights or trade secrets either with regard to content, or the way this content was structured in databases and computer programs. The right to profile transparency can be (partly) trumped by such trade secrets and intellectual rights of profilers. These rights potentially also pertain to data relating to users. In the present deliverable we will also have a look at intellectual rights in user generated content and data profiles. Profilers are not the only ones who possibly hold such rights in profiles; end-users can also have intellectual rights in parts or even the whole of their profile.

This deliverable provides a more systematic overview of the legal issues that are at stake in the context of IPRs and portrait rights of the OSN users. Compared to the earlier version of this deliverable (D3.3) we have made a clearer demarcation between the research in this deliverable and the research on IP rights on the side of OSNs (D3.7, the updated and adjusted version of D3.2). The current deliverable starts from an analysis of the law and adapts the structure of analysis outlined in deliverable 3.3. Whereas D3.3 only provided an initial outline of this analysis and a tentative first exploration of the topic, especially with regard to portrait rights and image rights, D3.8 will provide a thorough, systematic and full-fledged legal analysis, which will then be applied to the OSN situation. This analysis will look at the following things. First, the protected subject matter of copyright and portrait and image rights is fully analyzed and delineated and then applied to the user profiles on OSNs. Second, the scope of legal protection - the ‘protected acts’ - that these rights afford, are

elaborated upon and the consequences for the OSN situation are considered. Thirdly, we look at how users can contractually license particular uses by OSNs of their content protected by IPRs and portrait rights. In relation to the issue of licensing protected content, we explore the question how the fact that OSN providers have a different business model from “traditional” exploiters of copyright works (such as publishers, music or film producers) and that they offer their services to the user/author “for free”, i.e. not for a fee, should affect the particular licensing conditions. We will furthermore research how portrait rights can act as a ‘trump’ for OSN users who (unintentionally) have licensed away so many uses of their IP content that the inalienable core of their portrait right is infringed upon. Portrait right could ensure that there is a core of the intimate sphere (portrait right protection) which cannot be contracted away. Fourthly, related to this, we will provide a comparison of the added value of resorting to image and portrait rights in relation to data protection rights (and copyrights).

2. Copyright

In this section, we will have a look at the question whether copyrights could be used as tools of empowerment for users of Online Social Networks. We will first study the use of specific copyrightable content posted on OSNs, like pictures, texts, videos. Here, we will investigate a set of legal issues that we encountered while working on D3.4 (describing the legal coordination and integration in the second year of the USEMP project) and which require further research. According to the dual objectives of empowerment and compliance, the investigation here will also turn towards the content used by the Databait tools themselves. After this, we will investigate whether users can also exert copyright claims on their user profiles or even with regards to their larger "digital persona" on OSNs. Finally we look at how users (could) license OSNs with regard to their user generated content and their 'digital persona'.

2.1. User Generated Content

Some of the 'user generated content' (a status update, a video, a picture, etc.) that a user uploads on her OSN profile is protected by copyright. Whether an OSN user has copyright on a Facebook post, a status update, music, or an uploaded picture (so-called User Generated Content) is an empirical question that requires investigating the facts: can these be qualified as "original", that is, as an expression of the author's own intellectual creation?[1] A statement of fact like "today it is hot" is not likely to be protected by copyright. However, many posts and updates on OSN will be more than mere factual statements and contain some element of 'originality'. Thus one can broadly say that in order for user generated content to qualify as the protected subject matter of copyright, the subject matter should be "original" or the author's own "intellectual creation"[2] and reflect the author's personality[3]. More specifically, this is the case if the author was able to express her creative abilities in the production of the work by making free and creative choices[4]. The Court of Justice of the EU has played a major role in the harmonisation of the originality requirement and has in one case suggested some criteria to assess whether a portrait photograph was protected under copyright: "the photographer can choose the background, the subject's pose and the lighting. When taking a portrait photograph, he can choose the framing, the angle of view and the atmosphere created. Finally, when selecting the snapshot, the photographer may choose from a variety of developing techniques the one he wishes to adopt or, where appropriate, use computer

[1] Parallel to copyright, user generated content are themselves defined in terms of creative effort. A certain amount of creative effort has to be put into creating the work or adapting existing works to construct a new one; i.e. users must add their own value to the work. (Vickery & Wunch-Vincent, 2007).
[2] Infopaq International A/S v Danske Dagblades Forening, C-5/08, ECLI:EU:C:2009:465, para. 37.
[3] Recital 17 in the preamble to Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, *O.J. L 290 , 24/11/1993 P. 0009 – 0013 ;*
[4] Eva-Maria Painer v Standard VerlagsGmbH and Others, C-145/10, ECLI:EU:C:2011:798, para. 89.

software. By making those various choices, the author of a portrait photograph can stamp the work created with personal touch'"[5].

It should be underlined that the requirement of 'originality' (which needs to be fulfilled in order for content to qualify as copyright protected work) does not depend on having an extraordinary talent. Even a very badly composed piece of text, music or picture can be subject to copyright: copyright protection is not limited to artistic expressions of high quality or achievement. It suffices that expression of the author's "own intellectual creation" can be found. The CJEU had admitted that newspaper articles, even excerpts of merely 11 words, and portrait photographs could be protected (subject to the factual assessment of the originality condition by the national courts). The "user" should in the first place assess (on a case-by-case basis) whether a selfie or a comment posted on a wall can be protected by copyright is and, ultimately, should the author and the user hold different opinions, the court will decide on the matter.

In D3.4 we made an inventory (see table 1) of which content processed by DataBait could be protected by copyright (if the requirement of originality is fulfilled).

Facebook data potentially subject to IP rights	**Description**	**Possible IPRs**
user_about_me	Access to a person's personal description (the 'About Me' section on their Profile) through the bio property on the User object.	Maybe, user copyright (on content stories)
User_posts	Access to a person's posts on the User object	Most likely, user copyright / 3rd party copyright
user_photos	Access to the photos a person has uploaded or been tagged in. This is available through the photos edge on the User object.	Yes, user copyright / 3rd party copyright
user_status	Access to a person's statuses. These are posts on Facebook which don't include links, videos or photos.	Yes, user copyright / 3rd party copyright

Table 1: Data potentially subject to IP-rights (Based on Table B.1 in Deliverable 3.4)

Now that we have established the *subject matter* of copyright protection and concluded that some of the content (such as pictures, videos, status updates and posts consisting out of text) derived from an OSN profile can be protected under copyright, the second question we need to ask is who the *author* of this content is. Often the author will be the OSN user: this is so-called *user* generated content (UGC). However, on OSN walls it's fairly common to post a picture created by somebody else or quote from a work (a newspaper article, a novel, etc.). As shown in table 1, a user profile can thus also contain content protected by a third party copyright.

[5] Painer, ECLI:EU:C:2011:798, para. 90-92.

A third question is what the *scope* of copyright protection is. *Protected acts* under copyright are *reproduction* (Article 2 of Infosoc Directive 2001/29/EC) and/or *communication to the public* (Article 3(1) of Infosoc Directive 2001/29/EC). When user generated or third-party content is used as the basis for the derivation of additional information through an automated profiling process, this necessarily involves making copies (that is, *reproduction*s) of it. Thus, *any* profiler, whether a commercial OSN like Facebook or a scientific transparency provider like DataBait, performs the protected act of reproduction. In contrast, 'communication to the public' is not an inherent part of the profiling process but can be part of the wider service provided. 'Communication to the public' means that the UGC and/or third-party content is shown and/or made accessible to people who are not employed by the service provider. Communication to the public should be interpreted in a broad sense, and, for example, also entails posting (a link to) protected UGC on an OSN wall.[6] Consequently, for DataBait (and an OSN like Facebook) the crucial question is whether the protected content is only communicated in the *private* communication between service provider and user, or whether the content is *communicated to a public*. When we look at the latest version of the DataBait architecture the UGC is only communicated to the individual user of DataBait (e.g., there are no posts on the users wall). However, also during the final period of the development of DataBait we will continue monitoring if any changes in the architecture are made that would imply that the DataBait data are, next to their reproduction for the profiling process, also communicated to a public.

The fourth question is if the reproduction or communication to the public falls under an exception (for example, because the reproduction is only a temporary technical copy in the sense of Article 5(1) of InfoSoc Directive 2001/29/EC) which would make these acts legal even when no explicit license exists. The exception for temporary acts of reproduction is described in Article 5 (1) of InfoSoc Directive 2001/29/EC:

> "Temporary acts of reproduction […] which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
>
> (a) a transmission in a network between third parties by an intermediary, or
>
> (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance,
>
> shall be exempted from the reproduction right provided for in Article 2."

Some examples of temporary, technical copies which fall under this exeption are given in Recital 33:

---

[6] For example, the Belgian Supreme Court (*Cour de Cassation*, 24 June 2015, *docket number P.15.0194.F*, (Criminal Division)) ruled that posting a link providing access to a copyright protected work by posting it on a Facebook wall constitutes a 'communication to the public'. This does not fall under the exception for private use. "With its judgement the *Cour de Cassation* confirms its earlier established case law that the exception for private use should be interpreted restrictively and that also any communication to the public on social or other media that is potentially accessible for a wider non-identified public falls under the exclusive rights of a copyright owner." Meyer (2015) at: <http://www.lexology.com/library/detail.aspx?g=2c099119-ee59-45fe-8da7-92147e9145cc> [last accessed 12 January 2016].

> "The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own. *To the extent that they meet these conditions, this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use should be considered lawful where it is authorised by the rightholder or not restricted by law*". (italics ours)

In the final version of this deliverable (D3.12) we will explore whether the copies made during the DataBait profiling process fulfill all the conditions to fall under this exception, that is whether they can be qualified as (1) transient or incidental reproductions, (2) forming an integral and essential part of a technological process, (3) carried out for the sole purpose of a lawful use of the work, that is, a use authorised by the rightholder or not restricted by law, and (4) have no separate economic value on their own. Our first impression is that the three latter conditions are applicable to DataBait's processing, but that the first condition (that the copies are 'transient' ot 'incidental') can be problematic for DataBait. There is no definition of these notions in the InfoSoc Directive, but it seems the legislator was thinking of very temporary copies (maybe at most a few hours) in RAM (random-access memory), local cache memory, or a proxy server – and not the kind of storage (most likely at least several months) of data that occurs on USEMP's 'historical database' server. We will discuss the final DataBait architecture in more detail with the other USEMP partners in the remainder of the project, but it seems likely that the temporary technical reproduction exception will not be applicable to DataBait. Apart from the exception for temporary technical reproductions, it is up to Member States to decide whether other exceptions suggested by the InfoSoc Directive are included in their national law. The full list of possible exceptions is listed in Arts. 5(2) and (3) InfoSoc Directive 2001/29/EC). These exceptions include, for example, reproduction for private use, reproduction or communication to the public (with a proper reference to the author) for scientific or teaching purposes, quotations for purposes such as criticism or review, or use for caricatures or pastiches. Limitations or exceptions other than the ones named in Arts. 5(2) and (3) which already existed under national law before the Directive was adopted, are allowed provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community (Art. 5(3o)). While it is possible that DataBait's processing could be qualified under some of these exceptions (notably, the exception for copies for scientific purposes), it is beyond our capacity to check all national jurisdictions of DataBait users. This brings us to the fifth question that needs to be posed when considering the role of copyright in profiling OSN users: how can users contractually license a profiler (an OSN or another service provider like DataBait) to use their protected content and portrait rights for some uses (i.e., particular types of reproduction or communication to the public). A license is necessary when a profiler performs a protected act and no exception applies. One does not need a licence if there is no protected act or if the act is exempted. Moreover, licensing only solves the copyright issue with regard to *user*

generated content (i.e. content of which the OSN user is the author): obviously, a user *cannot* license a profiler to reproduce or communicate third-party content over which she holds no rights (e.g., a third-party picture, video or text posted on the user's wall). In relation to the issue of licensing protected content, we explored in D3.7 (and in D3.11 and/or D3.12) the question how the fact that OSN providers have a different business model from "traditional" exploiters of copyright works (such as publishers, music or film producers) and that they offer their services to the user/author "for free", i.e. not for a fee, should affect the particular licensing conditions. Another issue with regard to licensing that we explore (see section 2.3) is how IP licenses can be made more specific – in contrast to the 'blank cheque' type of IP license which is included now in the ToS of most commercial OSNs, which basically permit any use of the UGC. In this respect it is also very important to know the details of how DataBait uses UGC (e.g., What is the purpose of any reproduction and/or communication to the public? If there is a communication to the public: which public?) to prevent that the DataBait IP licence becomes as general as the one given to the OSNs (which is something we criticize – see section 2.3 in this deliverable).

As explained in D3.7 it is very unlikely that the USEMP consortium infringes on the copyrights of DataBait users in as far as they explicitly license the USEMP consortium. In the Data License Agreement [DLA] signed by DataBait users (see D3.6), a license is given to the USEMP Consortium Partners to use all data gathered through the DataBait Facebook app and the browser plug-in (clause B). In the current version (December 2015) of the DLA the license does not make any specific reference to the licensing of IP protected content to the USEMP consortium.. One reason why no explicit IP license was included in the first version of the DLA is that from the point of view of data analytics, IP protected data do not differ from unprotected data (e.g. raw data). Both categories can be equally interesting (or uninteresting) to perform profiling upon (see D3.7 for a detailed discussion of this issue): there is no added value to profiling based on IP protected content compared to unprotected content For example, while a post containing a factual statement ("20 degrees in Amsterdam today!") falls under a different legal regime in terms of IP than a post containing a trace of her authorship ("Oh rainy, rainy Amsterdam, which makes my heart go TOMTIDOMTIDOM – how I love your cloudy thunder"), both can be equally interesting to derive additional knowledge from (Where is the user located? What is her mood? etc.). The reason is that the use of data for profiling purposes is *not* based in their 'creative' or 'artistic' value. Similarly, for a DataBait user concerned about profiling based on her OSN data the distinction between IP protected and unprotected content might not be immediately intuitive. Thus, the current DLA simply describes which data the user allows to be used ('licenses') for the DataBait profiling, without distinguishing IP protected content from other data :

> "…data that You share on Facebook as well as data collected by the web browser. This data can be data You posted (volunteered data), or data captured by the USEMP tools (observed data). The latter concerns online behavioural data (storing what You did on the Internet and on Facebook)". (Clause A of the DLA, version December 2015)

The current DLA does not specify that the category of "volunteered data" can contain some IP protected content (notably user's videos, pictures and textual posts that bear some trace of 'authorship'). For the sake of transparency and legal clarity we will include a specific IP clause in a next version of the DLA. The exact wording of the IP clause in the DataBait Data Licensing Agreement is something which will be studied in more detail in the remainder of the USEMP project (which will be reported in D3.12 and/or D3.13). As discussed below, in

section 2.3, the DataBait IP clause will differ from the those contained in the Terms of Service of major OSNs like Facebook, which we consider too general and of which the legal validity is far from certain under the national copyright law of several Member States of the EU[7].

It is our impression that currently most Facebook apps that perform some form of user profiling, only ask permissions to *access* user data and not for a separate copyright license (i.e., a permission to *copy* the data for the purpose of profiling). Could one argue that the user *implicitly* licenses the app developer to copy her data, by installing the application? This seems an unsuccessful line of argument, given that most (if not all) national jurisdictions within the EU only recognize *express* copyright licenses to be legally valid. Another line of reasoning that a developer of a profiling app is likely to raise is that Facebook, who has received a license to sub-license all IP protected content from each user (see below, section 2.3), makes the data accessible through a Facebook app, and that this could maybe be considered as an implicit form of sublicensing of Facebook to app developers[8]. If one would follow this line of thought a user could not contest this sublicense and the fact that no direct agreement is signed between the app developer and the author of copyrighted material would not matter. However, this implicit sublicensing argument also seems highly problematic. Not only because there is no *explicit* ('express') IP sublicense Facebook gives to its app developers, but also because a Facebook user could contest (as we explain below, in section 2.3) the validity of the license she has granted to Facebook, based on the fact that it is too wide and unspecific. The validity of the Facebook IP-license has not been tested in any court yet, but it does not seem unlikely that an end-user could successfully contest the scope of her IP licence to Facebook. For USEMP and the DataBait tool this means that it is very important to include a separate IP clause in the next version of the DLA. DataBait end-users who don't agree to have their copyright content reproduced for the DataBait profiling purposes, should not be participating in the project – unless we conclude (we will report this in the final version of this deliverable, D3.12) that USEMP's processing of the copyright

[7] In a recent report the Norwegian Consumer Council analyses the terms of 20 mobile apps in order to uncover potential threats to EU consumer and data protection hidden in the end-user terms and privacy policies of apps. Norwegian Consumer Council (March 2016), *APPFAIL: Threats to Consumers in Mobile Apps*, online available at: <http://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps>, and <http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf >. On the fact that the ToS of dating app *Tinder* are challenged in court for being too general and vague: <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html>, <http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/AK_Kartellrecht_2015_Digitale_Oekonomie.pdf?__blob=publicationFile&v=2> and <http://www.euractiv.com/section/digital/news/member-states-swipe-left-tinder-under-fire-in-three-eu-countries/>.

[8] Depending on how she uses the app, a Facebook end-user provides permission to let the app developer *access* her data on instalment. All apps have access to 'public information' (name, profile picture, background picture), information of users that is publicly searchable for all parties. This access cannot be contested. While Facebook apps, when they are installed by the user, ask explicit consent for the *access* of any other data, they do not ask whether the user licenses the app developer to *copy*, *share* or *adapt* her copyright protected works. However, one could argue that the license to do so is *implicitly* provided by Facebook (who holds a license over all the IP protected content of the user and is free to sublicense it). The Facebook policy for app developers is unclear in this respect (only asking that cached data should be updated): https://developers.facebook.com/policy/ (accessed 1 December 2015).

protected content is limited to reproductions that are covered under the exception for temporary acts of reproduction (for the sake of extracting meta-data, i.e. information that is not protected under copyright; see our initial analysis above).

In the final version of this deliverable we will also look at the 'licening'-situation with other OSNs, such as Twitter or Instagram, which do not have an 'app'-platform like Facebook does.

Here we have to pose a question from the perspective of empowerment: does the fact that an OSN user holds copyrights in (some of) her user generated contents *empower* her towards the OSN? Profiling entails making some kind of copy (reproduction) of a work. Having copyrights in a work (either because one is the author of the work or because one has been licensed to use it) means that one is entitled to prevent others from making copies of the work, share it with others (though exceptions are often made for sharing within a small set of people) or adapt it (e.g. a text into a play or a film) – unless these uses fall under an exception (temporary technical reproduction, scientific purpose, parody, criticism, etc.) Copyrights are absolute rights and can thus be enforced against anybody (in contrast to, for example,a contract, which concern rights that can be enforced against the other party in the contract: a contract provides relative rights). In Europe, copyright for example lasts for the life of the author until 70 years after her death[9]. After this time, the work enters the public domain and is available to be used freely. A copyright holder could thus use her exclusive right to prevent profiling to take place based on her copyright protected content (see D3.7). This could be empowering. However, in the case of Facebook the copyrights of users do *not* empower them. Because of the all-encompassing IP license (see section 2.3 below) that users must grant to Facebook when signing up, the user seemingly cannot use her authorship over the works as a legal means to prevent Facebook from reproducing the content (for profiling purposes or any other purposes) or from sublicensing others to use (reproduce) the content. Things could become different if the validity of the license granted to Facebook was to be challenged and Facebook had to adjust the licensing conditions (see section 2.3 below).

Yet, for the time being, the fact that some of the 'user generated content' (a status update, a video, a picture, etc.) that a user uploads on her Facebook profile is protected by copyright does not empower her. But what about copyright on a profile as a whole, including the backend information available to the OSN provider, such as the machine readable behavioural data it captures?

2.2. User Profiles and Digital Persona on OSNs

Thus, the next question is whether user profiles themselves could qualify as copyright protected works and whether OSN users could claim authorship in them, or whether to the contrary, OSN providers can do so. Before starting the analysis, we have to first indicate what we mean by the word "***profile***". A profile can in a general sense be taken to refer to "an outline of something, especially a person's face, as seen from one side".[10] This general

[9] Art. 1 of Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights, OJ L 372, 27.12.2006, p. 12–18.
[10] Oxford Dictionary.

definition is useful to retain, especially later in this deliverable when we will make the link to the concept of the digital persona. In the context of online social networks (or on the web more generally) the term profile has acquired a more specific meaning of "a user's summary of their personal details or current situation".[11]

This definition is useful for our purposes. It emphasizes the fact that the user herself has provided the data with regard to personal details or current situation, which are visible on someone's personal page on an OSN. The user for instance often provides these personal details during the processes of signing up for the OSN during the registration process and these data can later become modified.[12] Data about current situation are often provided in the processes of actual usage of the OSN by writing posts, or uploading content, etc.[13] The term "summary" also indicates that the user profile that is visible on OSNs merely constitutes a limited representative model of details about this person. It only provides a part of the story and only contains a small part of the personal details that are available about a user. These additional details might for instance be available in public records, but also in offline social networks of friends and family. More relevant, such additional personal details also exist in online social networks themselves, without the user necessarily having access to them. This is due to the fact that OSNs track all kinds of behavioral data about users and derive data inferences on the basis of data mining exercises. This is why it is useful to not limit our analysis to the visible user profiles, but to also look at the larger ***digital personae*** that are pieced together by OSNs on the basis of different data sources: not just data actively created by the OSN user (registration data & page content), but also incidental data (information about a user derived from the behavior of other users), traffic data (logging data and browsing behavioral data), interaction data (likes and group memberships) and inferred data (data derived from any of the other data). Annex 1 provides a breakdown of the different data streams that make up the 'social ontology' of the digital personae of Facebook.

Clarke has defined the notion of a digital persona as "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual." (Clarke 1994). This definition highlights both the representational and operational aspects of digital personae: 1) they are a model of a person that is used for a certain purpose in a specific context (here in the case of OSN for providing services), 2) they function as a digital proxy for this individual on the basis of which certain actions are performed or withheld (by the OSN). Solove expanded the notion of the digital persona when he stated that "it is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital person composed in the collective computer networks of the world" (Solove 2004, p. 1). He has highlighted that the privacy problem in relation to these digital personae both stems from the paradoxical situation that these data are pervasive and cover large parts of our lives, but also have limitations in the way these data capture us and distort who we are (p.49). In this deliverable we will use this notion of the digital persona for the more encompassing analysis of a set of user data by predictive data

[11] *Ibid.*

[12] Few data will be protected under copyright at that point (except perhaps for a tag line or a personal description).

[13] Schneier calls these two types of data used in online social networks "service data" and " disclosed data" (Schneier 2010). In Annex 1, these are classed in one category ("registration data and page content"). The second type of data are more likely to be protected as copyrightable "works".

models: such 'user profile'[14] is constructed by an OSN from different data sources and serves as an operational proxy for this person in order to act or be acted upon.

Protected subject matter. In order to determine whether a user profile or the larger digital persona is eligible for copyright protection, we have to determine whether it can be qualified as a "***literary or artistic work***". For this qualification several questions have to be answered. First, can the profile be considered a "collection" or a database?[15] Second, is the profile an original creation? Third, who is its maker?[16]

At first sight it sounds like a rather awkward question: "Can a profile be considered a literary or artistic work"? One might ask what a user profile has to do with art or literature. We must however be reminded that we are here not dealing with common sense concepts, but with specialized legal concepts that have acquired their own meaning. The concept of copyrightable "work" has over time become extended to cover a range of different objects, including ones that seem to have to do little with art or literature.[17] For this purpose we can have a look at article 10 of the TRIPS Agreement:

> Article 10
>
> Computer Programs and Compilations of Data
>
> 1. Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).
>
> 2. Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.[18]

Databases are here likened to literary works for legal purposes and are thus included in the types of objects that qualify as copyrightable works (art 10 TRIPS). Article 5 of the WIPO Treaty determines that copyright pertains to "compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations".[19] This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation." In

---

[14] In D3.7 (section 1.4) we distinguished five 'objects' in a profiling process which can be relevant from the perspective of IPRs: the set of training and testing data, the algorithm which is 'trained', the hypothesis space, the resulting 'trained algorithm' (or: 'predictive data model' or 'classifier'), and the data analysed by the trained algorithm. Each of these 'objects' in the training process involve some element of 'labour' (sometimes 'creative' labour bearing a mark of authorship, sometimes 'just' the investment of time, money and mental energy) which the maker might wish to protect. When a predictive data model (or several predictive data models) is used to analyse a set of user data[14], this is called a 'user profile'. It should be noted that this is often a fragmented, gradual process: it is not necessary that at one single moment in time a complete 'user profile' is created.

[15] In this deliverable we will only be discussing issues of copyright on databases and not of the *sui generis* database rights. When it turns out to be useful, these might be discussed in deliverable 3.12.

[16] (Van Dijk 2009).

[17] The best illustration of the wide variety of different works is provide by article 2 of the Bern Convention for the Protection of Literary and Artistic Works, 1886 (1967). These also include 'compilations' or 'anthologies' (art 2(4)), which are helpful for user profiles when users are compilers of their own profiles.

[18] Agreement on Trade Related Aspect of Intellectual Property Rights (TRIPS) of 15 April 1994, Marrakesh.

[19] WIPO Copyright Treaty (WCT) of 20 December 1996, Genève.

Europe this subject matter is covered by the Database Directive.[20] The object of protection – the "database" – is here defined very broadly. Article 1(2) defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means". We will thus have to investigate whether profiles could be qualified as ***databases*** that are protected by intellectual rights.

Applied to our case, we could say that profiles are: essentially (1) a collection of different data (in the sense distinguished in Annex I), (2) which are independent of each other due to the way they are ordered as distinct entries in the profile format.[21] The data that make up the collection are also (3) systematically or methodologically ordered according to the data types or categories that make up the profile. The collection – to qualify for IPR protection under the database copyright – must thus satisfy these three criteria. Nevertheless, the fourth condition, which requires individual access to the data out of which the profile is composed might be more problematic. We have to distinguish here between the empirical perspective of the OSN user and the technical perspective of the OSN provider. In a trivial empirical sense the OSN user will have individual access to her profile data with regard to the visual part of the user profiles of OSN sites like Facebook and Twitter. Here all the data that make up the user profile like registration data, page content, interaction data and incidental data (see Annex I), are individually represented and accessible. Nevertheless, this is different for the larger invisible profile of a user: the larger inaccessible digital persona. It is of course possible to use access requests to OSN providers in order to endeavor to obtain such data. Based on European data protection law, OSNs would be required to provide access to all personal data processed. While such access will arguably shed light on additional parts of the user profile, it still does not provide us with a full picture. It has been shown that in case of such access requests only partial data of the larger data profile relating to a user are provided.[22] Whether OSNs fulfill their informational duties towards the data subject with such partial access will depend on a balancing of their rights (e.g. trade secret protection) against the informational rights of the data subject (see D3.7). It could moreover also be asked whether a request-based structure qualifies as "accessible" in the sense of the Database Directive and thus whether it can qualify as a copyrightable database at all. This question should probably be answered affirmatively, since the criterion of accessibility is rather technical in nature: the way the database is built should allow someone to access the data. For this, it is thus irrelevant whether a user can factually access her data profile or not, the criterion is not user-centered. As an OSN provider, Facebook can technically access the data and this is sufficient for satisfying this condition. The fact that Facebook can modulate such

[20] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[21] There is requirement however that the data should be pre-existent to the creation of the database (ECJ, 9 Nov 2004, C-203/02, British Horseracing Board v William Hill), which is not the case with OSN's. The OSN's basically decide upon the ordering template which then becomes filled in with data by users, the OSN or third parties. Some of these data are indeed pre-existent such as uploaded content like videos and images, or some personal data entered in registration processes. Other data however are created on the spot like posts, behavioural tracking and data inferences.

[22] http://www.zdnet.com/article/facebook-the-law-reasonably-states-you-cant-have-all-your-data/. In terms of the data types that make up the digital persona on OSNs (see Annex 1)., we could say that these access requests still omit browsing behavioural data, many incidental data and inferred data. For the differences in results between the Facebook "download your data" tool and a legal access request, see: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html; http://europe-v-facebook.org/EN/Data_Pool/data_pool.html

access to users might even be proof that we are dealing with a database in the sense of copyright law. Something similar may be said about the fact that it can select certain users based on specific characteristics (derived from the user's activity) for advertisement purposes.[23]

In any case, when we presuppose that the question whether a profile qualifies as a database or compilation of data is answered positively, one has to determine whether the "selection or arrangement" of data constitutes an "intellectual creation" in the sense of copyright law. Here we stumble upon the question of *originality* of profiles.

The criterion for originality has been harmonized in Europe in the Directives for copyright protection of computer programs[24] and databases[25]. Article 3 of the Database Directive determines that originality requires a certain "selection or arrangement" of data, which constitutes the maker's "own intellectual creation". In the *Infopaq* judgment the European Court of Justice has further extended the harmonization of this criterion to the regime of copyright in the European Union in general.[26] In order to satisfy this criterion, it is necessary for the maker of the database to select or arrange the data in her own manner. This implies that she has had the possibility to make choices during the creation process and that the way that these creative possibilities have been used constitute sufficient personal contribution to the shaping of the profile. We have to determine whether this is the case for users in the creation of their OSN profiles. For the criterion of 'arrangement' this is questionable. Through the design of the user interfaces, OSNs like Facebook and Twitter offer the user a preset format for data entry that the user fills in. This does not, or barely, leave the user any creative space for choosing the way these data are systematically and methodically ordered. The OSN layout does not provide for any flexibility for "arrangement" in this regard. In this sense the criterion of '*selection*' of data leaves more creative space for the user. The user does have a wide margin for self-expression through an ever more personal selection of data (pictures, status updates, videos, notes, newspaper articles, etc.).[27] The question is whether such selection constitutes the user's 'own intellectual creation', bearing her 'personal stamp'. On OSNs this is almost per definition the case. OSNs are tailored for reflecting your personality through your online actions. It could however be questioned how much creative activity can really be found in this.[28]

Ownership. After the question whether an OSN user profile or digital persona is eligible as an original work (like a database) that can be protected by copyright and the determination of the scope of protection, we have to discuss the question of ownership: Can the user be considered the ***author*** of these possible objects of copyright? To start with, we have to distinguish this question of the authorship of OSN *user profiles* or the *digital personae*, from the question about the authorship of the *contents* that might make up these data

[23] In case the data profile would not qualify as a 'database' in the sense of the directive, one might turn to the less stringent criteria for "compilations of data" of article 5 WCT, article 10 TRIPS and article 2(4) of the Berne Convention mentioned above, or even to the general criteria for a work of literature or art.

[24] Article 1(3) of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs.

[25] Article 3(1) of Directive 96/9/EC

[26] ECJ 16 July 2009, C-5/08, Infopaq).

[27] See also D3.3, section 2.3 on this.

[28] This points at a larger problem copyright law is facing, because of lowering its standards of originality due to the incorporation of ICT technologies like databases and computer programs.

compilations. This question has been dealt with before in section 2.1. Secondly, authorship of the user profiles or digital personae must also be distinguished from the authorship of the databases and software programs that have been used to derive data that have fed into the digital persona model. These questions have been dealt with in deliverable 3.7. We are here interested in the question regarding the authorship of the digital persona itself.

The distinction between the visible user profile and the invisible parts that are added by OSN's once again becomes important here.[29] Large parts of the visible user profile have been assembled by the user either by filling in data through the registration process, by uploading content and by writing text. Apart from the data posted on the user's personal page by other users, the data suggested or filled in by the OSN or affiliated third parties like advertisers, the user can thus be said to be the maker of this data compilation and may be able to claim copyright.[30] The user can however not be said to be the author of the invisible structure of the digital persona relating to the data about her generated, gathered and stored the OSN provider (*e.g.* behavioral data and inferred data, See Annex 1). Even when these data might be personal or sensitive in the legal sense, for copyright purposes they cannot be considered the user's creation. They are rather created by the OSN provider. The OSN provider also assembled these data together with other data sources (registration data, disclosed data, incidental data, interaction data) in an encompassing data collection that constitutes the digital persona of the user. We have already remarked above that the OSN provider chooses the preset format for data entry for the categories of registration data and disclosed data to be filled in by the user. A similar argument pertains to the preset entry format for incidental data filled in by other users, and to the types of relational actions that the OSN platform affords the user to take (membership, commenting, tagging, liking, checking in). In this way the OSN provider can be said to "arrange" all these data in a systematic and methodic way (even if it does not "select" all of these by itself, but leaves this to users) and thus satisfies the copyright criterion of originality for databases. OSN providers can thus more likely claim copyright in the more encompassing data arrangement that constitutes the user's digital persona on OSNs. These rights are distinct from any rights the OSN might have in the software executing this arrangement, or the data thus arranged.

It becomes apparent that the question whether the user might have any database copyrights on their OSN digital persona has to be scaled down and limited to a sub-collection of this overall data compilation, namely the visible user profile. Does this partial approach to databases legally make a difference? Not necessarily. The European Court of Justice has determined that a sub-collection of data can also receive legal protection as a separate database as long as it satisfies all the relevant legal criteria. It has stated that "where a body of materials consists of several separate modules, it is necessary […] to determine first whether that module itself constitutes a database within the meaning of Directive 96/9".[31] In this sense each of these sub-modules might in itself constitute a separate database when by itself it fulfils all the conditions for database protection. In addition it has to be determined whether this separate database fulfils the criteria for copyright protection laid down in Article 3(1) of the Directive.

---

[29] For simplicity sake we will omit in this analysis the data added by third parties, for instance due to actions like tagging, friending, etc. This is what Schneier has called incidental data (Schneier 2010).
[30] Although IP clauses might apply here in favour of the OSN.
[31] ECJ, 5 March 2009, C-545/07, Apis v Lakorda, §62.

Scope of protection. If the copyright requirements for databases are met, the author can exercise four kinds of exclusive rights: the right of temporary or permanent reproduction of the database or parts of it; the right to translate, adapt, arrange or alter the database; the right to distribute the database to the public; the right to communicate, display or perform the database to the public.[32] Furthermore, apart from these patrimonial rights, copyright law also grants the author of the work certain non-patrimonial rights, called "moral rights" that cannot be transferred away in the way the economic rights can. These moral rights include the right to be attributed as the author of the work and the right to the integrity of the work which prevents the work from being distorted, modified, or mutilated.[33]

It must be added however that all these rights only pertain to the structure of the database and not to its contents. This means that on the basis of copyright on databases the contents might be extracted, but that the way they are selected or arranged may not be appropriated. In our case, this would imply very little protection, since it means the data in the profile are free to be reutilized and recombined in new data mining attempts.[34] Nevertheless, some of the user's economical and moral right in the profile might pose certain limits to such data re-combinations and thus offer some legal protection. This might be the case when (OSN) operations of data addition or data derivations can be qualified as a translation, adaptation, (re-)arrangement, alteration, or distortion of the original form of the user profile.[35]

Summarizing this section, we could thus conclude that it is of little avail to turn to copyright for empowering users with regard to their digital persona in OSN's. Apart from the question whether digital personae constitute copyrightable works as databases, which we tentatively answered positively, several other questions were posed. First, copyright in databases might offer relatively little remedy against the copying and recombining of individual data entries. It merely protects the form in which the data are combined and in this sense merely offers some protection when data re-combinations create derivate works of the original profile, or affect its integrity. Second, users could only exert rights on a very small part of their digital persona, namely mainly the visible parts of the user profile. They thus merely have a partial claim that is not enough to cover control over the larger digital persona, especially the parts that are invisible to the user and which are gathered by the OSN. This is mainly due to the specific structuring of copyright law which points the analytic lens with which the lawyers look at these technologies at the process in which a technology is created (instead for instance at the consequences of a certain technology, which is an analytic lens that privacy law provides) in order to determine who its authors are.

---

[32] Art. 5(a-d) Directive 96/9/EC

[33] Article 6bis of the Bern Convention for the Protection of Literary and Artistic Works, 1886 (1967).

[34] The reproduction of the arrangement of data that constitutes the visible user profile is often wanted by the user, because it is necessary in order to use the OSN (for instance for checking her time line). An interesting question is whether the thus arranged database is communicated to the "public". Is the user the only one who sees the selection, or can a significant group of other people check her profile and see her selection?

[35] An important aspect the moral right to integrity is that the work is protected against unauthorized changes, because of the intimate tie between the subject matter and the holder of the right benefiting from the legal protection (the same applied to the personality right to one's image to be discussed in the next section). This could perhaps be applied to cases in which the representation of the model in the user profile or digital persona is not accurate (I am considered an unhealthy person on the basis of the available data, but in reality I am very fit).

2.3. Licensing copyright protected content and profiles

Can licensing copyright protected content or copyright protected profiles empower or disempower the OSN user?

Let's first have a look at the licensing database copyrights in one's 'digital persona'. This is, of course, a rather unexplored field because the whole idea of a copyright in a 'digital persona' is very novel. Nevertheless, in as far as a 'digital persona' is just a particular type of database, there are some things that can be said about its licensing. As explained in the previous section (2.2) a digital persona is not just the compilation of postings by a user, but the entirety of the profile available to and compiled by the OSN provider. An OSN user obviously cannot license database copyrights which are not hers: that is, she cannot license the parts of her digital persona covered by database copyrights of the OSN: the OSN's *arrangement* of the user generated content (UGC) and the 'invisible' database of *additional data* 'created' or 'derived' by the OSN from this UGC. However, the user might have database copyrights in the 'visible' parts of her digital persona (that is, in her self-created 'user profile', in as far as she has not only authored the *individual content* but also, at least partly, the *content as a collection*: i.e., its arrangement and assembly in a particular way). Such partial database copyrights, limited to a sub-collection of the overall data compilation constituting her 'digital persona', can be relevant for the empowerment of OSN users. If it is established that the user has *some* right in the database, licensing matters. For example, a user may want to accept reproductions and communications for certain purposes (communicating with friends) but not for others (e.g., extraction of metadata to be sold to third parties or to serve ads).

This also means the OSN user could license her partial database rights in her digital persona in exchange for a fee, though it is doubtful that commercial parties would be willing to pay for it, and the fee would be very low. One could argue that empowerment is not related to the height of the fee: micropayments could have their own sense of empowerment and the fee could be more a matter of principle than of substantial remuneration. However, it seems to us that user empowerment through exclusive (partial) database rights would be rather based in how the aforementioned scenario that these rights can be used to *prohibit* certain uses (cf. the protection of "authors" under certain copyright laws), than in the *licensing fee requested to permit* certain uses.

Of course, OSNs like Facebook could try to extend their already extensive IP license to also cover the digital persona of OSN users. This would disempower the user even more. However, as we argue below, even the legal validity of Facebook's current IP license[36] on user content is highly doubtful – and so would any extension of this license to cover database copyrights on one's digital persona.

After having looked at the licensing of database copyrights in one's digital persona, we turn to the second point: the licensing of copyrights in individual content, especially with regard to Facebook. This is not as speculative as the licensing of one's digital persona and is therefore discussed by us in more detail. In Article 2 of the *Facebook Statement of Rights and*

[36] Article 2 of the *Facebook Statement of Rights and Responsibilities*[36] (version of January 30, 2015). Online available at : <https://www.facebook.com/terms>

Responsibilities[37] (version of January 30, 2015) every Facebook user gives a non-exclusive, transferable, sub-licensable license to Facebook to use any IP content that the user posts on or in connection with Facebook. This means that, as a Facebook user you continue to be the copyright holder over your own IP content[38] and that you can license others next to Facebook (the license is non-exclusive). However, Facebook claims the right to reproduce, publicize and distribute the user's copyrighted material and the right to license it to others (the license is transferable, sub-licensable and worldwide) – and, finally, Facebook stipulates that the user cannot claim royalties over any of this. This could mean, at least in theory, that Facebook could sell a user's pictures to an advertiser who uses them in an ad campaign or reproduce that user's status updates in a hard copy book. However, this might violate privacy or data protection rights and if done on a massive scale, could create public outrage and bad publicity. Nevertheless, selling UGC from OSNs like Facebook is a serious business model – if not for Facebook, then at least for some third-parties[39].

Art. 2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)
4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).

[37] Online available at : <https://www.facebook.com/terms>
[38] The matter is more complicated where users share works to which they do not hold the copyright, such as pictures, news articles or videos.
[39] An example of such third party use of UGC is the 'Piqora'-app, built on top of UGC photos that are sold for advertising (<http://www.piqora.com/>).

5.	We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

One could debate whether the formulation of Art. 2 of the *Facebook Statement of Rights and Responsibilities* is in accordance with copyright law. One major problem from the persective of copyright is that Art.2(1) does not specify a purpose specified for the IP-license granted by the user to Facebook. This is in line with the analysis of Wauters e.a. (2014), who argue that Facebook's IP-clause lacks specificity and is thus not in accordance with Belgian law[40]. It is doubtful whether under general contract law and consumer law, it is valid to have a reciprocal contract where the value of one's obligation is as unknown and uncertain as in Facebook's Ip-clause.

However, if we assume, for the sake of the argument, that the IP-clause is legally binding, what would this imply? Most contemporary data analytics ("data mining" including "profiling") involve the need to *copy* data in some way before one can extract information from it (Triaille et al, 2014). We know that a user's Facebook profile may contain expressions protected under copyright, such as status updates or pictures she has made. Making a copy of such works (e.g. downloading them to one's server in order to analyse them) is to *reproduce* the works, an act that requires the author's prior consent[41], i.e. the Facebook user's consent. This may even concern a third party where the Facebook user has "posted" works from another author[42], which is only allowed when the copyright holder has allowed one to do so ("given you a license"). Even though there are authors (Triaille et al, 2014) who argue that there should be an exception to copyright protection for technical copies made during the

[40] "For instance, under Belgian law, there are strict rules that have to be taken into account when licensing copyright to a third party. For each mode of exploitation the remuneration, the duration and the geographical scope has to be determined.65 Also, it is not possible to transfer rights for modes of exploitation that do not yet exist at the conclusion of the contract.66 Given the broad scope of the provision in Facebook's Terms of Use, this clause would most likely not be enforceable under Belgian law". (p. 267)

[41] It is good to note here that this also implies that the way in which some popular (image) search engines work -gathering documents (images/texts) without specific consent of the web sites and/or authors- can be problematic from a copyright perspective if no exception applies. For example: there have been several cases in Germany re Google Images. In 2003 the regional court in Hamburg ruled that Google infringed on copyright, but in 2008 the same court ruled in a similar case that Google's thumbnails should be considered 'fair use'. See for an analysis of the trends in court decisions in some national jurisdictions in the EU: <http://www.law-right.com/the-hidden-liability-of-google-images-in-copyright-infringement/> However, all depends on the particulars of a case. Particularly when search engines reproduce and/or communicate content (without having a license) for *commercial* purposes, this could constitute a copyright infringement.

[42] Unless such copies could be exempted under the exception of "temporary reproduction", but the list of conditions is rather strict: see Article 5 of the Copyright ("InfoSoc") Directive. Exceptions and limitations

1. Temporary acts of reproduction […], which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

(a) a transmission in a network between third parties by an intermediary, or

(b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

process of (scientific) data analysis (see deliverable 3.7), such an exception currently only exists in Japan and the UK. This makes Art. 2 of the Facebook *Statement of Rights and Responsibilities* very important: because it gives Facebook, and third parties licensed by Facebook, the right to make copies of the user's IP content - including copies made for the sake of the automated extraction of information (although this is not explicitly stated).

However, as mentioned above, a very general copyright license clause ("a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook") is not valid under all national copyright laws. The rules on copyright contracts have not been harmonized at the European level, hence national legislators are free to impose specific requirements for copyright contracts, especially when the author/natural person is involved. Yet Facebook offers only this all-or-nothing approach to its users. Admittedly, Facebook users have immediate control over the use of their "content": they can control who has access to their profiles, status updates, photos, images and all other matters they wish to share with their friends or the public in general. Also, Facebook allows the users to delete content or their account and according to Facebook's IP license the authorization ends at that time. Nevertheless, it is hard for the user to check whether Facebook effectively deleted the content, though legally speaking Facebook can no longer claim the copyright, due to its own stipulations. However, during the entire period that the user keeps her account and posts copyright protected creations, Facebook benefits from its large IP license. Consequently, it is not possible for the user to distinguish – in terms of her licensing - between the types of use or the purpose of the use that could be imagined. Thus, the concern is not so much whether content can be effectively deleted but rather whether it is exploited in a way that is not mentioned and not known by the user; Facebook could argue that the user knows that the content is saved on the servers for the purpose of operating the OSN (communicating with friends), even serving ads (visible to the user) but not other uses (for example, extracting meta-data that will be 'traded', more specifically 'hashed'[43], to others). Because the IP license is so vague it seems that everything and anything goes.

This is not due to the "nature" of copyright: copyright licensing offers an excellent possibility to be very specific about what one's data can be used for, by whom, for which period of time. One could easily imagine – in analogy to the various types of creative commons licenses – how a user of a browser or social network would benefit from the option to license her copyrightable work through (a possibly standardized yet refined) licensing agreement in which it is specified exactly for what period, what kind of copyrighted works ("data") could be used for what purpose. Here the author could, for example, state that Facebook can only sub-license her work in relation to – say – cancer research or that she does not want her protected content to be mined for the purpose of commercial consumer research. Licensing

[43] Hashing is a form of matching pseudonomized information: "Facebook has developed what's called a "hashing" system that converts things like phone numbers and email addresses to a jumble of digital data. Its partners, such as DataLogix, use the same system to anonymize phone numbers and email addresses captured in the real world. The trick is that the hash of a phone number captured on Facebook will look just like the hash of the same phone number captured in a brick and mortar store, so the two companies can match the numbers without actually trading them". From : <http://www.wired.com/2014/12/facebook-knows-ads-influence-offline-purchases/>

could as such be a very effective tool to offer users of social networks and browsers a possibility for some granularity (and thus user-empowerment) in deciding what is allowed with their creative productions. We should take into account that, due to the business model that currently informs most commercial OSNs, such empowerment assumes that users have a bargaining position in relation to the OSN. If an OSN simply refuses such granularity the empowerment remains a dead end. We note, however, that the GDPR – discussed in D3.6 – contains a new stipulation for consent in the proposed art. 7.4:

> "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller"

This entails that a 'powerful' service provider cannot require consent for the processing of personal data that are not necessary for the service provided; such consent must be freely given and this means that the service providers cannot deny the service to those who decline consent for data processing beyond what is necessary for the service. This provision could be leveraged for negotiations regarding the copyright on content processed for purposes other than the provision of the service.

The fact that a service is rendered for 'free', that is without direct financial remuneration from the user, does not change the fact that the business model of OSNs is commercial and money is being made. As argued by Wauters e.a. (2014), the commercial nature of the OSN entails that the terms and conditions under which this service is rendered should be in line with general contract law, and as fair in terms of data protection and compliant with consumer regulation as any other commercial service. Complying with general contract law, data protection law and consumer regulation does not make it impossible to pursue a commercial interest. Nevertheless, the fact that the service is 'free' is of interest in a different respect, namely how this affects licensing conditions. This question is further explored in deliverable 3.7 (and its successor, D3.11), which notably inquires into how the fact that OSN providers have a different business model than "traditional" exploiters of copyright works (such as publishers, music or film producers) and offer their OSN to the user/author "for free", i.e. not for a fee, should affect the particular licensing conditions. The question has been raised whether a far-reaching non-exclusive license can be granted on the basis of a non-specific clause in the general terms and conditions of an OSN (without defined object, scope of rights, duration). Under many European copyright laws[44], copyright licenses with the author have to meet certain requirements (as a matter of substance or for evidence purposes). The ratio for such specific copyright contract rules is generally to offer more protection of the author, who is considered the weak party in a negotiation with a professional party that will commercially exploit the work. The question to be explored in more detail in the next (and final) of this deliverable (D3.12) is whether OSN providers exploit IP-protected content in a way which differs from "traditional" exploiters (as they exploit 'banal' content on an aggregated level: not for the 'artistic' qualities of the content but in order to sell targeted advertising space and/or ameliorate their data models of users) and offer their OSN to the user/author without requesting a fee. An additional question already touched upon in D3.7 is whether this data-based business model changes the equation in favor of the OSN

[44] In the following version of this deliverable, D3.12, we will look into this in more detail.

provider[45], resulting in a lesser protection for the user/author. If this question is answered positively (which, according to us, would make sense) this could result in licensing conditions which are not as general and vague as they currently are in Facebook's Terms of Service, but are also less strict than in the case of traditional licensing contracts. We will probably elaborate on this in the next version of this deliverable (D3.11) and experiment with the best possible formulation in the IP clause[46], which we will add to the Data Licensing Agreement. It seems important that a data controller, like Facebook, who mainly needs copyright licenses in order to be able to profile users (and not for any traditional publishing of the content) should be more upfront about this in the copyright clause. In the DataBait DLA we will make clear that our IP clause does not relate to any traditional exploitation of the content of the user, and only relates to reproductions made for the sake of profiling.

An important problem with the idea of granular licensing of copyright content on OSNs is that the difference between protected and unprotected works is neither relevant from the perspective of the OSN-profiler, nor from the perspective of the profiled data subject. The data subject may not want to be profiled – independent of the question whether the content is 'original' or not. The profiler has the same indifference for the distinction: an 'original' picture of breakfast cereal (with a touch of 'authorship') is not better or worse for the purposes of profiling than a picture of breakfast cereal lacking originality (and thus copyright protection). Moreover, the OSN will probably have difficulty distinguishing copyrighted works from unprotected content in an automated way (this would require a data model to distinguish 'original' works from non-original ones). Thus, while copyright protection in combination with granular licensing conditions could empower the user with respect to copyright works, enforcing it would be difficult in practice and would not solve the problem of being profiled based on content which does not fall under the protective scope of copyright – which is the majority of the digital trail of an OSN user. We thus have to conclude that the empowerment based on licensing of content is limited.

[45] Article 16 (the freedom to conduct a business) of the EU Charter of Fundamental Rights might be of relevance here as well : "The freedom to conduct a business in accordance with Community law and national laws and practices is recognised".

[46] It should be noted that the IP clause in the Facebook ToS is not very comparable to the IP license of the USEMP DLA : these are very different licenses, notably because USEMP is not a commercial enterprise. However, the analogy with Facebook is made here to underline that USEMP should not have a license which is as general as the one of Facebook.

3. Portrait Rights

We will now turn away from intellectual rights for purposes of user empowerment and direct our attention to a different legal field: the field of 'image' or 'portrait' rights. We will explore whether portrait rights can be used as a 'trump' for OSN users over some of the intellectual rights of OSNs. This is part of the "logic of rights trumping each other" as has been explained in deliverables 3.1-3.3. Here it was mentioned that the different strands of legal research – data protection rights of the OSN user, trade secrets and intellectual rights by the OSN, and portrait rights of the user – "relate to each other as a sequence of cards, where each consecutive card could trump the previous one". In a similar way in which data protection rights by the OSN user like the right to access to one's data can be curtailed by trade secrets and intellectual rights by OSNs, the latter protection could also be trumped by the portrait or image rights by OSN users. Due to their status as a personality right, image and portrait rights ensure that there is a core of legal protection that cannot be contracted away.

By turning to image and portrait rights we also leave behind the popular idea of 'owning one's data'. As we have seen before, many of the data types that make up one's digital persona (behavioral and inferred data, or even incidental data) are not created or made by the user, but by the OSN itself. The user thus does not 'own' these data. On the other hand, and this is what we will try to explore here, this does not mean one is without legal avail. The user does have other rights in these data: apart from the data protection rights dealt with in deliverable 3.6, the user might also exert image rights in her digital portrait. In this sense the field of image or portrait rights provide a curious mix of property and personality thinking, blending together in this phenomenon of "the commercial appropriation of personality" (Beverley-Smith 2008).

In this section, we will explore this possibility by addressing two questions. First, are image or portrait rights at all applicable to profiles or digital persona on OSNs? This is not a straightforward issue and without a confirmative answer, we can forget about this trump card. Second, we need to inquire whether portrait or image rights offer added protection for the data subject compared to the regime for the protection of personal data.

3.1. Digital Portraits on OSNs?

Deliverable 3.3 introduced portrait rights and set out to apply portrait rights to content posted on OSNs and to digital personae on OSNs. Here we refine and further elaborate on this proposal. As a start, we need to clarify the tools of our analysis by making a distinction between "portrait rights", "image rights" and a general "personality right". A 'portrait right' is a very specific legal term that can be found in copyright legislation of some EU member states like the Netherlands and Belgium ("*portretrecht*"). For example, Art. 20 of the Dutch Copyright law (*Auteurswet*) states that when…

> "…a portrait is commissioned by the person portrayed, the person who owns the copyright on the portrait is not allowed to publish that portrait without the consent of the person portrayed (or when this person has died, without the consent of her surviving relatives in the ten years after her death). Art. 21 Auteurswet states that if a portrait has been published by the artist who did not create that portrait under the commission of the person portrayed, the publication thereof is illegal insofar as it

> infringes a reasonable interest of the person portrayed." (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010, p. 195)[47]

From this quotation, it becomes clear that portrait rights on an image in which someone is depicted can function as a restriction on the exercise of copyright on that work by its copyright holder.

In the Anglo-Saxon world this right is known as the "*right to one's image and likeness*". In French it is called a "*droit à l'image*", in German a "*Recht am eigenen Bild*" and in Dutch "*recht op afbeelding*". Although these 'image rights' might be considered the equivalent of portrait rights, they are somewhat broader in scope, forming the superset of which portrait right are a subcategory.[48] This is reflected in the fact that in France and Germany they are enshrined in the general civil code.[49] Due to their incorporation in copyright law, portrait rights are generally evocable in case the relevant portrait is a work of copyright.[50] Image rights do not have this limitation and other limitations that we will discuss hereafter. For these reasons, we will hereafter broaden the scope of our analysis to image rights more generally. We will still refer to portrait rights when the precision of our analysis requires us to do so.

Image rights are a rather undetermined legal notion. Image rights are considered to be based on a general personality right, which can be derived from Art. 8 ECHR or national constitutional rights such as Art. 1 of the German Federal Constitution.

> "Persönlichkeitsrecht, in Germany, is a widely recognized doctrine, based on the constitution and on laws, but primarily defined and emphasized in German case law. 'Based on these Articles and sections 823 and 826 of the Civil Code (Bürgerliches Gesetzbuch - BGB) the German Federal Court, has developed a "general right of personality" known as Allgemeines Persönlichkeitsrecht. Under the general right of personality one can find a number of different rights such as the right to one's image, the right to one's name, and the right to oppose publication of private facts. As opposed to the U.S. law there is no specific right of privacy recognized in German law but privacy rights are covered by this general right of personality. Some of the rights protected under this principle are also protected by specific provisions in the law such as section 22 of the Art Copyright Act (Kunsturhebergesetz—KUG).' (Van der Sloot 2015, p. 26)

There is no harmonized EU legislation on image rights and so different approaches exist between different European countries. The main differences are related to the UK, French and German approaches. In the common law tradition of the UK there is no unified conception of an image right, but rather a cluster of different torts such as 'passing off', defamation, breach of confidence (as a form of privacy protection) and appropriation of personality. These torts developed over time through judge-made law, rather than through

---

[47] Article of the 10 Belgian Copyright Act has a similar determination.

[48] In this sense there is thus a continuity between both rights (De Hert and Saelens 2009). The distinction made in this deliverable is maintained for reasons of analytic clarity, since, as will be argued, in some regards both rights have different scope and thus different consequences.

[49] Nevertheless, Germany also has its own version of portrait rights called "Rechte an Bildnissen" or "Porträts", enshrined in article 22 of the Kunsturhebergesetz.

[50] Whereas in Belgium this is a rather strict rule (Voorhoof, pp.153-154, citing the case of the Court of Brussels, 12 March 1996, AM 1996, 449), in the Netherlands this is less so. See for instance Dutch Supreme Court, 22 May 1916, NJ 1916, 808; Dutch Supreme Court, 22 November 1966, NJ 1967, 101.

legislation. In the civil law traditions of the European continent, image rights are considered a full-fledged right and are often enshrined in statutory law. The right is often based on the fundamental right to respect for private life, or the right to personality. This 'privacy' aspect is what is called the dignitary or *non-patrimonial* side of image rights: issues that relate to the protection of the autonomy or personhood of people. On this aspect, in spite of some differences, one could speak of a certain European "common core of personality protection" (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010). The case-law of the European Court of Human Rights (ECtHR) also has a harmonizing effect in this regard (Synodinou 2014). In its landmark judgement in the case of *Reklos and Davourlis v. Greece,* image rights were first held to occupy a special position among other privacy interests. The court formulated this as follows:

> "A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image." (EHtCR, 15 January 2009, 1234/05, §40).[51]

Nevertheless, there is much less agreement on the *patrimonial* aspect of image rights: the recognition that the use of someone's image for commercial purposes should also be legally protected. This 'publicity' side of image rights has much more affinity with property approaches or intellectual property rights like copyright and trademark law.[52] With regard to this patrimonial aspect, there are for instance important differences between French law and German law and we can thus not speak about one unified legal field here.[53]

Protected subject matter. The next question we need to pose, is what we mean by 'portrait' or 'image' in the sense of this legal field? First, it needs mentioning that the technical way – the medium – by which the portrait is made is irrelevant.[54] Whereas initially historically, the notion typically referred to images in the sense of painting and drawing (or sculpture), over time due to the introduction of new communication technologies, the notion has become applied more broadly to a number of other objects, like photography, film and television. Nevertheless, these representations are limited to the "visual arts" (Dierickx 2005, p. 62). The important criterion for determining whether a certain image deserves legal protection is whether the person depicted can be *recognized* or *identified*. For this purpose a broad "test of identification" is used (Pinckaers 1996, pp. 129-133; Dierickx 2005, pp. 66-74) that involves several criteria. First, the portrayed person does not need to be identifiable from the perspective of strangers, but also from the perspective of persons who know her. Second, direct or immediate identification is not necessary, but closer investigation and comparison is also possible and other circumstances than the portrait (name, family, clothing, surroundings, origin, distribution of non-anonymized version of the image) can play a role here. Most typically someone would be recognized by an image of the face, but this is not necessary. One could also be identified by other distinctive elements. In some court cases it has for instance been determined that, in spite of the fact that the face was not visible in its entirety

[51] See also ECtHR, 7 February 2012, 40660/08, von Hannover v. Germany (no. 2), § 96.
[52] Although copyright law also recognizes the moral rights of the author, not just the commercial ones.
[53] French law has a dual system with a dichotomy between privacy and property interests, whereas German law takes a unitary approach to these (Synodinou 2014).
[54] This phrase even occurred in the original article (18) on portrait rights in the Dutch copyright law of 1912, but was later taken out. See also Dutch Supreme Court, 2 May 2003, NJ 2004, 80.

on the image, other characteristic elements like haircut, color of hair, body silhouette, posture, clothing style, could still identify the person.[55] This foregoing that the test is mainly visual in nature, but also entails (simple) cognitive comparative elements.

Over time, several non-image elements like signature, name, nickname and voice have also been granted a similar protection as portraits in the case-law of several EU member states.[56] The criterion of recognizability and identifiability are also central here. There is also discussion about whether a fictive personage could qualify as such, when it can be tied either to the one who impersonates it (the actor, artist)[57] or the one to whom it refers, is based upon or inspired by[58]. Furthermore, in German law a work like a novel or a film could even be

> "derogatory to the whole biography and character of X and therefore of serious intensity. In cases such as this, German lawyers do not speak of a sole violation of a person's right to honour but of a violation of a person's biography (*Lebensbild*), consisting of all actions, sentiments and convictions which constitute a person's individuality or identity. The right to one's biography may also be called the right to protect one's individuality or identity against false, misleading or incomplete biographical details. This right is affected in cases in which a fictitious character can be identified as a real person by her or his relatives, friends or by the public."[59] (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010, p. 214)

It thus becomes clear that there is a whole range of distinctive elements by which a natural person can be identified and that have been granted similar protection as portraits. For this reason, (Pinckaers 1996) has even argued for shifting the attention from the term portrait, which has more limited applicability, to that of *persona* as the object of legal protection. This is an interesting proposal for our present exercise. This move would probably imply a shift from portrait (and image) rights to personality rights more generally.

Application. Now we have to pose the question whether these rights are applicable to user profiles or digital personae on OSNs? Do these constitute 'portraits' or 'images' of the user in the sense of these legal regimes? We mentioned that the technical way the portrait is made is largely irrelevant for the application of portrait rights. As we have seen, these rights have been typically applied to images in printed media like newspapers and journals, but also later, with the development of communication technologies, to film and television. In this sense digital media form a next step in this evolution. Nevertheless, they are both limited to the "visual arts" and thus to representations that can be mainly visually recognized. Although it might seem that this makes it applicable to several elements of OSN profiles like photos, videos or posts, we must remember however that we are no longer looking at individual user-generated data, but at the larger structure of the profile itself. This more encompassing data

---

[55] HR 2 may 2003, NJ 204, 80 (Breekijzer); Vzr. Rb. Breda 24 june 2005, AMI 2005-5, nr. 14 (Gouden Gids & Katja Schuurman vs. Yellow Bear).
[56] These can be considered as different personality rights from *image* rights (Dierickx 2005, p. 55).
[57] Rb. Amsterdam 26 March 1981, KG 1981, 40; BIE 1983, nr. 32, p.81 (Max 'n Specs). See the comment in (Pinckaers 2009, p. 37).
[58] (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010, pp 206 ff.)
[59] Something similar may be said of French law. "Even without using his/her name, the identification of a character in a novel can result from a collection of concordant indices, such as the place where the story occurs, professional similarities, the recitation of notorious facts, etc. […When] one could clearly notice the similarity between [someone's] life and career and that of the character in the novel [, one could] prove that the author was inspired by the life of X to write the novel." (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010, p. 212).

model mostly includes non-image types of data. When we for instance look at the data types mentioned in Annex 1, only the page content data literally contain such image data.

Nevertheless, the important test behind this legal regime was whether the represented person could be identified in the image by (a combination of) distinctive traits. This test also applied to non-image related elements. Pinckaers' thus proposed the term *persona* for the set of all distinctive characteristics, visual and non-visual, that identify a natural person. When we apply this notion to the online context of OSNs, we get very close to the notion of the *digital persona* as defined by Clarke as a digital model of a person. Moreover, Solove's notion of the digital person as an 'electronic collage' of a person's life" (Solove 2004, p. 1) comes very close the digital version of the German image right notion of the *Lebensbild* as the person's biography that consists of all actions, sentiments and convictions which constitute a person's individuality or identity. This can also essentially be said about digital persona created on OSNs, which focus exactly on constituting the digital biography of a person, of all her actions (posting, uploading), sentiments (mood analysis[60]) or convictions (like political and religious views[61]) all biographically placed on a person's 'timeline'. Furthermore identification is indeed an essential trait of profiles on OSN. The personal data entered during the registration for an OSN are essentially tailored towards the goal of identifying the natural person behind the profile and thus relating later data to this person. Furthermore also indirect information like inferred and behavioral data are essentially tailored towards subsequently recognizing somebody as the same person as before, or as being a certain kind of person befitting a group profile.

On similar grounds, Roosendaal concludes that "the digital persona is also an image of an individual, albeit in the form of an entire data set and not a picture or video (although these may be part of the data set)" (Roosendaal 2013, p. 243). On this basis it could be argued that image rights can be applied by analogy. The digital persona on OSNs of a user could then be qualified as his or her digital portrait in the sense of the law.

Scope of protection. In most jurisdictions, the right holder of a portrait or image right is granted a series of actions. The most important is the right to prohibit the *publication* of the image without the consent of the person represented. This 'right to prohibit' constitutes the core legal action of both portrait rights and image rights. There is however an important divergence between the actions granted by both legal regimes. Image rights here also offer a broader scope of protection. Whereas portrait rights only allow the right holder to prohibit the publication of the portrait, image rights also include the right to prohibit the *making* of the portrait without consent of the portrayed person.[62] Furthermore, in contrast to portrait rights, in the case of image rights the right to prohibit is not limited to publication alone. This right extends to 'the *illicit usage* of the personality of the represented person' and the '*exploitation* of the image for commercial purposes' without the person's consent (Bertrand 1999, p. 137), (Dierickx 2005, p. 87).[63] This focus on commercial use in general of the image provides for quite a large scope of legal action. To the contrary, portrait rights offer no protection against the making or reproduction. The phase of making the portrait is here thus irrelevant, it is

[60] (Kramer, Guillory, and Hancock 2014).
[61] (Kosinski, Stillwell, and Graepel 2013). See these derivations made in USEMP in deliverable 6.2.
[62] (Voorhoof 2009, p. 155), (Dierickx 2005, pp 85-86).
[63] This is not limited to acts of publication, but also extends to acts selling, giving and putting in the possession of someone (Dierickx 2005, pp. 92-96).

rather the moment of marketing the product that determines whether a legal action can be instituted (Pinckaers 1996, pp. 136-137).

This broader position of image rights is also reflected in the *Reklos and Davourlis v. Greece* case mentioned above. The ECtHR here stated that

> "Whilst in most cases the right to control such uses involves the possibility for an individual to refuse publication of his or her image, *it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person*. As a person's image is one of the characteristics attached to his or her personality, its effective protection presupposes, in principle and in circumstances such as those of the present case, obtaining the consent of the person concerned *at the time the picture is taken* and not simply if and when it is published. *Otherwise an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image*" (EHtCR, 15 January 2009, 1234/05, §40, our italics).

Application. When we presuppose that user profiles or digital persona on OSNs qualify as 'portraits' or 'images', we can first ask whether they have been published by the OSN. On first sight, there seems to be a rather straightforward binary answer to this question. The visible user profiles have been published, whereas the invisible parts of the digital persona are not. This easy division has to be qualified however. With regard to the visible user profiles on Facebook, users can tweak the settings of who gets to see what. Thus a user can nowadays choose between the categories 'public', 'friends', 'family', 'only me' (or 'custom'), thus progressively narrowing the circle of people that get to see the relevant data. It might be clear that profiles without privacy restrictions (with the setting 'public') qualify as public in the sense of portrait law. For the other settings however, it will have to be determined in each case whether the concrete group of people that has access to the profile will constitute a public in the sense of portrait law. This is difficult to say, since the case-law predominantly deals with classical printed media, or sometimes television and film aimed at large audiences.

Since the image right to prohibit publication is part of the general personality right enshrined in Art. 8 ECHR, inspiration might be gotten from privacy law, which has more experience with such 'digital publics'.[64] In this sense it is relevant to turn to criteria derived from an Opinion of the Article 29 Working Party on Online Social Networking. In this Opinion the working party stated that "When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere." Moreover, even when the user does confine her profile to self-selected contacts, "In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know. A high number of contacts could be an indication that the household exception does not apply." (Article 29 Working Party 2009, pp. 5-6). When we reason by

[64] We can also turn to copyright as the other cited foundation for these rights. Copyright law might be especially relevant for the interpreting the notion of publication in portrait right law (rather than image rights), due to the fact that these rights have been enshrined in copyright statutes. Copyright law grants two publication rights to the copyright holder. These are the right of "communication to the public" and the right of "making available to the public", the latter of which is especially relevant for publication and transmission on the internet. These two rights are enshrined in article 2 and 3 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

analogy, in the case of portrait and image right on OSN profiles this would imply that a user profile with the privacy setting 'friends' could be considered public ('published') when the user has befriended a large indistinct amount of people who have access to her profile. With regard to the invisible digital persona on OSN the answer seems plainly negative. No one apart from the OSN itself has access to this, not even the user herself. There might be an intrusive, privacy-related dimension to the use of the portrait, but this is not so much related to the outgoing side of the portrait, the presentation of this personal information to the public, which is the case with classical portrait rights cases, but rather to the incoming side so to say: the fact that the user receives advertisements based on her profile. In this sense the digital portrait is never made public and portrait rights in the strict sense offer little remedy. This might change however when we switch to the broader category of image rights. These rights also offer protection against the making of the image and thus the moment and process in which the image was created, even before it is published. This "also covers the individual's right to object to the recording, conservation and reproduction".[65] According to the court such an essential attribute of one's personality would otherwise fully be in the hands of a third party without the individual having any control over it. This defensive, more privacy-related formulation seems more suited for digital persona on OSNs. Facebook indeed records all kinds of data about our behavior, either through behavioral tracking or by deriving such data through inferences. It further stores and thus conserves these data on its servers. Also, the data is mostly entirely in the hands of Facebook, without the user barely having control over them. Lastly, what is interesting about image rights is not only their privacy aspect of resisting infringements on someone's personality, but also the commercial side. As Bertrand stated, these rights in this sense offer broader protection against the illicit use of the personality or exploitation for commercial purposes. This is exactly the case with Facebook, who uses the digital personae of the user for commercial purposes for obtaining advertisement revenue.

3.2. What is the Added Value? Comparing portrait and image rights to data protection rights

After spelling out the nature, criteria, scope and exceptions of portrait and image rights and applying these to digital profiles on OSNs, we now have to face the inevitable question: Are portrait and image rights an interesting option for user empowerment? Do they add anything to the protection and guarantees offered by privacy and data protection law? From the perspective of empowerment, it might be interesting to compare image rights to data protection law. Both legal regimes have interesting similarities, both in protected subject matter – the test of identification - and in the scope of protection – the right to prohibit or object. This is in part due to their strong relation with the right to privacy (art. 8 ECHR).

In the section above we have mentioned that the definition of the protected subject matter of portrait law – the portrait, depends on a test of identification (and recognition). The same is true for data protection law. Article 2(a) of the Data Protection Directive (95/46/EC) personal data are defined 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

[65] EHtCR, 15 January 2009, 1234/05, *Reklos and Davourlis v. Greece.*

particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". So we see that the identifiability of a certain natural person due to certain indices, also plays a crucial role for determining whether we can speak of personal data in the sense of data protection law, just as it does in portrait law.[66] Nevertheless, one could argue that this test tends to be more visual in nature in the case of image rights than it is in data protection law, where the identification typically takes place through the use (or combination) of all kinds of identifying data, which can also be done by a computer. However, this difference -if existing at all- is not very large; data protection law does not specify the means through which the identification takes place and this can also be a very visual.

A similar thing might be said about the role of anonymization. Due to this test of identification, the application of portrait law finds its limit of applicability in anonymous or anonymized images. Nevertheless, this identification does however not have to be direct and on first sight. Closer investigation may result in identifiability, which is also the main criterion for applicability of data protection law, taking note that such identifiability may be either direct or indirect. Furthermore, practices to anonymize the portrait by for instance covering the eyes of someone with a black bar, do not necessarily preclude identification.[67] As might be clear from what was written above, other identifying traits could also perform the same role. Here there is another link with data protection law. Data protection law is also not applicable in case of anonymous or anonymized data. Nevertheless, in the quotation above, we can see that 'indirect' identification should also be taken into consideration. This makes it important to consider the possibilities of re-identification of anonymous data. In this context, the Article 29 Working Party, in a recent Opinion on anonymization techniques, pointed out "the inherent residual risk of re-identification linked to any technical-organizational measure aimed at rendering data "anonymous"" (Article 29 Working Party 2014a). There is no general metric to determine such anonymity in advance, but that it rather depends on the proceeding state of the art of the research in the field. This implies that additional new information or algorithmic techniques (for singling out, linkability or drawing inferences) could eventually permit the re-identification of a previously anonymized piece of data and thus cancel out the effect of anonymization.

In this context it also deserves mentioning that article 4.3b of the GDPR introduces the new notion of 'pseudonymisation' defined as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person." While it should be underlined that pseudonymous data are personal data in the sense of data protection law, this concept is situated between the rather black or white dichotomy between ordinary, non-pseudonymised, personal data and anonymous data and rather functionally deals with the risk and likelihood of identification of an individual. With regard to the example mentioned above, this implies that hiding someone's eyes with a black bar may render this person anonymous for one party but as long as some other party can attribute the image to the individual by connecting it to additional information, the data is considered

[66] See also (Roosendaal 2013, p. 243) on this similarity between DP law and portrait rights.
[67] Court of appeals Amsterdam, January 14, 1993, AMI 1993 (*former champion lightweight*), discussed in (Pinckaers 1996, pp. 131-132).

pseudonymous, not anonymous. This concept might also be relevant for portrait or image rights.

The second point of comparison between image rights and data protection law is the scope of protection: the right to object and the possibility to withdraw consent. Article 14 of the Data Protection Directive grants the data subject the *right to object* at any time to the processing of data relating to her. Although this right is of a general nature, it especially pertains to situations in which this processing is necessary in the pursuit of the "legitimate interests" of the data controller or third parties to whom the data are disclosed (article 7f DPD).[68] Such interests can include quite different things ranging from broad societal benefits to more narrow economic interests.[69] The objection by the data subject made in these circumstances has to be made "on compelling legitimate grounds". These have to relate to the particular situation of the processing of personal data (article 14.a DPD). Nevertheless, such a high standard is not required in case the personal data are or will be "processed for purposes of direct marketing" by the data controller or by a third party to whom these data will be disclosed and by which they will be used (article 14.b DPD). Here the Directive specifically states that the data subject is offered the right to object to such disclosure and use without additional conditions and free of charge.

[68] Data protection law and image rights can also be compared on this point with regard to the notion of "balance of interest". Article 21 of the Dutch copyright Act for instance determines that the portrayed person can oppose the publication of her portrait when her "reasonable interest" opposes this publication. In subsequent case-law, courts have determined that such interests classically mainly included a privacy related interest as related to the right for one's private life of article 8 ECHR. Later a commercial interest of the portrayed was also recognized in relation to the commercial exploitation of the popularity of a person. These requirements will have to be balanced with other important interests, mainly a public interest in protecting the freedom of speech in a democratic society. See (Pinckaers 1996, pp. 139-140), or (Synodinou 2014, pp. 189-191) for image rights more generally. In data protection law we can see a similar balance of interest in article 7f, which states that a data controller can process personal data when this "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". Notice however that in this situation privacy is considered an "overriding" interest with regard to the legitimate interests a data controller might have, which, as we have seen before, could also be of a mere economical nature.

[69] "The nature of the interest may vary. Some interests may be compelling and beneficial to society at large […]. Other interests may be less pressing for society as a whole, or at any rate, the impact of their pursuit on society may be more mixed or controversial. This may, for example, apply to the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services." (Article 29 Working Party 2014b).

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Article 7

Member States shall provide that personal data may be processed only if: […]

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Furthermore, the e-privacy directive that deals with location data and traffic (meta-) data relating to electronic communications[70], adds that "users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time" in case of the provision of value added services or marketing services (article 6.3, 9.1 E-PD). This explicit possibility to withdraw consent is also valid for data protection law when personal data are processed, but implicitly, since it is not mentioned in the Directive (Article 29 Working Party 2011). This might change however when the new General Data Protection Regulation comes into force. The latest proposal by the Council of the European Union on the 11th of June 2015, contains an article 7.3 which states that "the data subject shall have the right to withdraw his or her consent at any time."[71]

[70] 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.

[71] Which does still not preclude the possibility of processing of the data on the other grounds mentioned in article 7, like the legitimate interests of the data controller mentioned above.

We can compare the right to object to the right to prohibit in image rights. We have already seen that the subject matters of these legal regimes overlap due to the nature of identification that the relevant information offers. Both regimes also seem to offer similar remedies to the right holder. As described above, image rights grant someone the right to object to the making and usage of the image in which she is portrayed, especially in a commercial context. We can thus summarize and in a very general sense state that both regimes offer the legal subject (data subject or the portrait/image subject) a right to object to the use of information that identifies her.

In the light of this comparison, we can thus proceed to ask what is the added value of the use and application of portrait or image rights for protection on OSNs in relation to data protection law?

Firstly, we have to explore whether the fact that an image right is a *personality right* offers advantages over rights derived from data protection law.[72] A personality right has an absolute, non-patrimonial, inalienable character (Dierickx 2005, p.2). The absolute character entails that it offers legal protection against everyone (*erga omnes*) and for instance not just against the one who created the image.[73] The non-patrimonial character entails that the image is not reducible to monetary valuation and that it does not belong to someone's patrimony.[74] The inalienable character entails that it is impossible for someone to transfer her image rights away to someone else, and also imposes limits to contracts where the exercise of image rights is waived. The image right holder can never lose all competence to exercise this right, neither by contract, nor by other means: a person can grant somebody else permission to use the image, for instance by license or contract, but this does not mean she loses all competence with regard to this image. This has important consequences, since it implies that this permission is always precarious and can always be revoked.[75] This means that an image right can be of help when a user has licensed away too much of her intellectual property rights.

From the perspective of data protection, which is itself a fundamental right but not a personality or moral right, the added value is less clear, because consent (Art. 7(a) of DPD 95/45) is never absolute – the proportionality of what the data subject consents to always has to be tested[76] (Article 6.1(c)requiring that the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;: consent can thus never be given for irrelevant, disproportionate an excessive processing) and moreover consent can always be withdrawn (Art. 7(3) of the GDPR). Finally, Art. 7(4) states:

---

[72] The potential added value of the personality rights resides in the capacity of the person to force the user to provide transparency on intended use and to oppose such use – in a way more economic rights are incapable of ensuring. The reason for this should be sought in the invasive nature of the new technology (parallel with photography when it first appeared) and the circumstance that the image outlives the moment of capturing the person in the image (which is thus beyond her control).

[73] This absoluteness however does not imply that this right cannot be overruled based on a balancing act, like the balance of legitimate interests we have seen in article 7f DPD.

[74] This does not preclude that image rights *also* have an important patrimonial side in addition to this non-patrimonial side, as we have remarked before.

[75] Although such revocation may of course have consequences, since the user might have to compensate the OSN.

[76] However, see Bygrave & Schartum (2009), who find that consent is not subject to a proportionality test.

> "When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract".

We have seen that *consent* could also be *revoked* in data protection law. Nevertheless, it has been more implicit[77] here, which has offered more uncertainties about the meaningfulness of this possibility in law and practice.

Furthermore and more importantly, consent is not a perquisite for the processing of personal data. It is merely one out of six legitimate grounds on basis of which personal data may be processed according to article 7 of the data protection directive.[78] If another ground has been chosen, withdrawal of consent is thus an ineffective option.[79] Image rights do not have this limitation, but can always be invoked against anyone (absolute character). However, this 'advantage' of image rights over data protection rights should be nuanced, as the right to object (based in data protection law) does not depend on which ground is chosen. Yet, the fact that image rights are a personality right makes them a strong (even if only complementary) right next to data protection rights: it makes it impossible for a user to waive the exercise of her rights based on a contract with an OSN composed by clever lawyers. With regard to user licensing, image rights could be even more valuable. As personality rights they would guarantee that there is an inalienable core of the intimate sphere that cannot be contracted away. This core goes back to the fundamental right to privacy as protected in article 8 of the European Convention of Human Rights. This can be of use in situations where people end up saying: "I did not understand the consequences of what the exercise of the rights I was waiving. Moreover, the one cannot consent to uses that did not exist and could not be foreseen at the time of signing.[80] However, again, the same goes for the fundamental right to data protection. Just like you can sell your economic right but not your moral right, you cannot sell your right to data protection. When you license the use of your data, you cannot, for instance, allow a data controller to deny that these data are personal data that relate to you; just like you cannot allow a person or organization to deny that you are the author of a text.

There is also an interesting link with copyright that might be instructive on this point. Copyright law also provides a mix between on the one hand so called moral rights that are inalienable and cannot be transferred away (the right to integrity and the right to paternity/attribution of the work) and on the other hand economical exploitation rights (like

---

[77] An interesting point concerns the time frame of the consent – see art. 7.3 GDPR. In D3.12 we will explore if this is different with the image rights.

[78] It must be said that consent is not the only ground for image rights either. In cases of public persons (politicians, celebrities) a balance has to be struck between image rights and right to the right to information of the general public (ECtHR, 24 June 2004, 59320/00, von Hannover v. Germany). Furthermore, now that the freedom to conduct a business has also been recognized as a fundamental right in article 16 of the Charter of Fundamental Rights of the European Union, OSNs could perhaps rely on this right in a similar balancing exercise.

[79] See (Curren and Kaye 2010).

[80] Whereas monetizing the image rights is to a certain extent a valid legal transaction; it is subject to conditions with regard to predictability. The question is whether, or to what extent the "portrayed person can actually foresee the use that will be made of the image and what impact this use might have.

the right to make reproductions, the right to distribute the copies of the work or to communicate it to the public) that can be the subject of contracting. Moral rights limit what you can contract away and the ways in which a contract can be composed. It is not possible to generally agree with any type of use in advance, for instance when later it turns out that certain changes provoke detriment to the honor and reputation of an author. One cannot transfer rights and can only waive future uses of a work in very limited ways and definitively not when this occurs in very general wording, merely when this has been specified very precisely.

The scope of protection of the *right to object* is also broader in case of image rights. We have seen that under data protection law this right is generally limited to objections based on 'compelling legitimate grounds', which is a quite stringent condition. Although this condition did not apply in cases of direct marketing, which is the situation most relevant for OSNs, image rights do not have this limitation.[81] They can thus be invoked in other cases that the images are used or other ways in which they can be exploited for commercial purposes.

Secondly, image rights seem to offer more *holistic* legal protection with regard to the protected subject matter – the digital persona - both in relation to copyright law and to data protection law. We have seen in the section on copyright that users only have a partial claim on a small part of their digital persona related to the visible parts of the user profile, but not on the larger digital persona gathered by the OSN of which most parts are invisible to the user. In fact the OSN itself has all kinds of intellectual rights in this larger dataset that they created themselves, including some of the data relating to these users. Deliverable 3.7 explores in more detail this mirror side to this investigation: the IP rights of the OSN on the (invisible) parts of the digital persona. From the user perspective this could be disempowering, especially when these rights are used as additional arguments by the OSN for not disclosing such data even after explicit requests for such access have been made by users.[82] This is one of the reasons why we have turned to image rights, or, in this case, portrait rights more specifically. We have seen how portrait rights are specifically suited as empowerments against the exploitation rights of copyright holders.[83] Applied to our case, this makes these rights suitable to be used against the copyright claims by OSNs on the digital portraits – the large profiles and digital persona - of users.

---

[81] Contractual responsibility may be an issue here however. If one has consented to the use of an image and afterwards the authorisation is withdrawn, the publisher (or other user) may suffer damage it wants to see compensated. It is a different matter when the publisher has used the image beyond the boundaries of consent, then there is no consent and a different legal ground may be required (e.g. freedom of expression or even right to conduct a business).

[82] There are examples of Facebook denying access request for user data based on the arguments of having trade secrets or intellectual property rights in the computer programs used for processing these data:
http://www.zdnet.com/article/europe-versus-facebook-the-law-protects-program-logic-not-data/,
http://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/. It must be mentioned however that this position was based on a faulty interpretation by Facebook of recital 41 of the data protection directive that states that the exercise of the data subject's right to know the logic involved in the automatic processing of data concerning him "must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information". A balance thus has to be struck. (Hildebrandt and Van Dijk 2012).

[83] This is how they are for instance enshrined in the Dutch and Belgian copyright Acts in which it was stated that "the person who owns the copyright on the portrait is not allowed to publish that portrait without the consent of the person portrayed" (article 20 Dutch Copyright Act).

Image rights can also be seen to offer more holistic legal protection when compared to data protection law. Data protection has become highly atomistic and specific, cutting the problem at hand up in a series of technical questions of concrete data processing operations and the rights and obligations with regard to these. It could be asked whether this toolbox sufficiently addresses the problems emerging from the taking together of different data streams from different sources: which larger OSN profiles emerge from putting these information streams together? In this sense image rights might offer an interesting addition that keeps track of the more holistic dimension of the problem by looking at the digital images of a user that arise when different sources of data are combined (See Annex 1).

Thirdly and more tentatively, the Databait tools might also provide us with a technological argument to mobilize the image right argument in digital portraits on OSNs. As we have argued, one of the big disadvantages of the larger digital persona of users on OSNs is their invisibility and inaccessibility, whereas it is the main unity of commercialization of someone's personality online. This invisibility makes it more difficult to substantiate what this digital persona is exactly and thus makes it more problematic to mobilize legal qualifications of these datasets as a digital portrait of the user. Here is where the Databait tool might come in handy. Through the user interface offered by the web platform (https://databait.hwcomms.com/welcome), many of the different types of data that normally remain invisible to a user are here represented together in the user profile of the Databait account (See Figures 1-4 hereunder). In terms of the data typology of the digital persona on Facebook provided in Annex 1, we could for instance say that: Databait's "My Disclosure" tool provides the user with insight into her "inferred data"; Databait's "audience influence" tool visualizes the user's "incidental data"; and Databait's "user tracker" tool visualizes some of user's "traffic data" (like cookies and trackers). In this way this tool digitally fleshes out the idea of digital portraits that we are speaking about there.[84] This portrait can be seen as an 'educated guess' of OSN portraits, generated from the same kinds of sources as the ones on OSNs and based on the same state of the art data mining algorithms. We will further investigate these points in deliverable 3.12.

At this point we have to counter a potential but interesting objection. At present OSN users do not know exactly in which ways they are profiled and what kinds of digital portraits are made of them. Legally this implies that the users are not well informed about these portraits and that they can thus not be said to have provided informed consent for their use. The moment however that DataBait starts providing its transparency tools to users to provide insight in this dimension, OSNs could argue that Databait users, on top of having accepted the OSNs terms and conditions, are also informed about what happens to their data. They have thus provided consent and this consent can be considered to be informed. Since they can no longer raise this legal ground against OSNs, this could actually make DataBait users worse off in terms of legal protection compared to non-Databait users! We have to ask however what counts as being informed here. The information that Databait provided merely tells us something about the general data components of the system that are being brought together and shows us in practice how this is done and what kinds of results can be obtained. Nevertheless, Databait does not tell us what concrete information exists about us

[84] A caveat has to be made however. These latter two tools only present but a very small part of all the incidental and traffic data (as described in Annex 1) and can therefore not be considered reliable windows on these parts of the digital personae of OSN users.

in the digital profiles of the OSN as it does not try to reverse engineer the data processing practices of OSNs. We don't know anything about our concrete file. This concrete type of knowledge about which data are stored and processed however is essential for exercising data protection rights, like the right to object. In this sense, the objection of being sufficiently informed cannot be raised against Databait users.

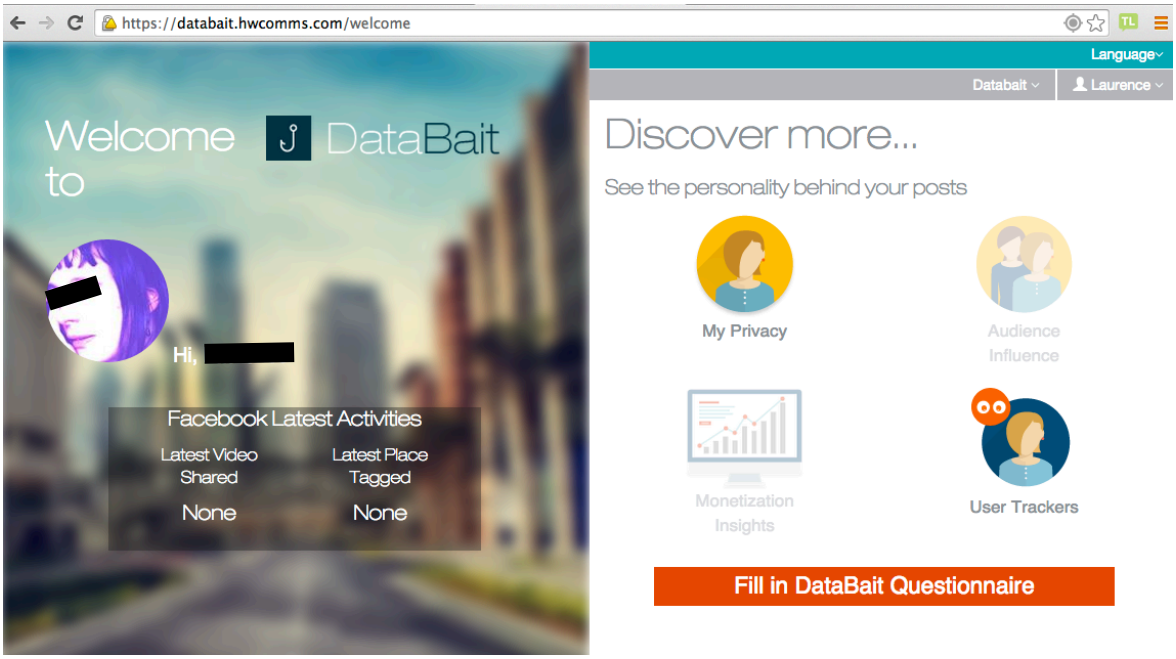

Figure 1. Welcome page of DataBait website (https://databait.hwcomms.com/)

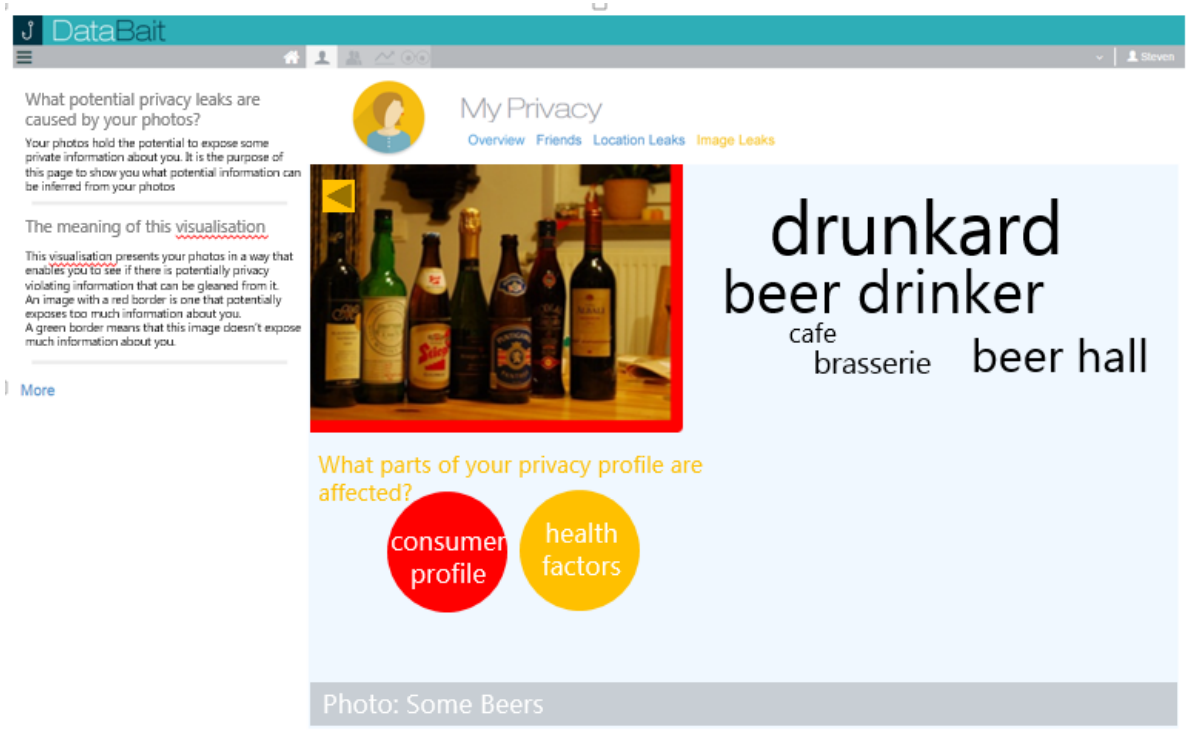

Figure 2. "Image Leaks" page in the "My Privacy" section on DataBait website.

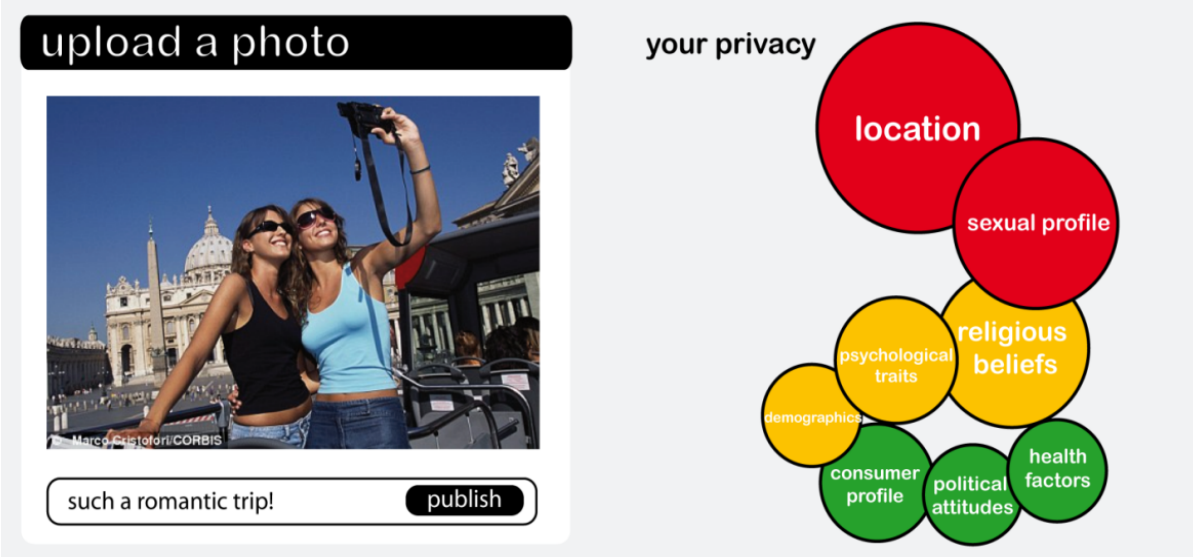

Figure 3 Visualization of the 'My Privacy score' (https://databait.hwcomms.com/)

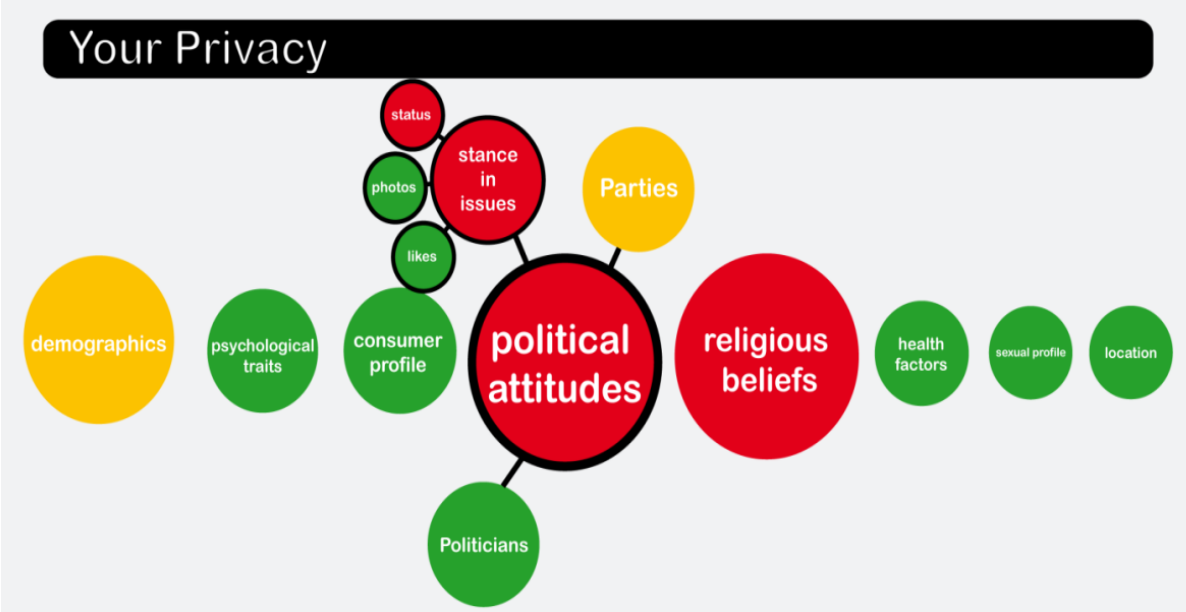

Figure 4 Visualization of the 'My Privacy score' (https://databait.hwcomms.com/)

4. Conclusion and Next Steps

In In this deliverable we analyzed the rights that might pertain to user profiles on Online Social Networks (OSNs), in order to find alternative forms of legal user empowerment with regard to their OSNs data. We especially focused on the holistic dimension by a shift in attention to the broader digital personae that are made of users on OSNs by bringing different data streams together. Two legal regimes were analyzed for this purpose: copyright law and portrait law.

It turned out that copyright law is of little avail to users in this context. With regard to content, users currently often license all their rights away (see e.g. the broad Facebook IP license), although this happens in ways that are often not legally valid. Even though we advocate licenses with more specific licensing conditions and a granular approach ("the license only allows reproductions for the following purposes :…"), in practice this would be difficult to effectuate. Moreover the distinction 'copyright work' versus 'unprotected content' is not very useful in the context of profiling. With regard to the empowering potential of copyright in profiles our conclusions were also rather pessimistic. This was mainly due to the fact that, when applicable, copyright claims would merely be applicable to the visible part of the user profile that the user has created. It doesn't provide any rights in the invisible parts of the larger digital persona that are assembled by OSNs. These data are the creation of the OSNs themselves and they can in fact claim database rights in these compilations. Copyright could thus rather work disempowering in these contexts, since such intellectual rights could actually be used against users who want access to their data.

For this reason we turned to portrait rights and image rights to explore whether they could be mobilized by users as a trump over some of the intellectual rights of OSNs and to claim some kind of control over their digital persona. Whereas the application of these rights to such digital portraits could be argued to work, it is definitively a speculative interpretation. But even if this application would fail due to the misfiring of some of the legal qualifications of the concrete components (if "usage" is for instance interpreted along the lines of some kind of publication), it is important to retain the general *raison d'être* of these legal regimes: to give the person who can be identified in a certain representation some kind of control, especially over the commercial exploitation of this representation including intimate features of the person portrayed, by granting her a right to object against such use. This is essentially the case with the way digital personae are used on OSNs. In this sense there are certain parallels with data protection rights. Nevertheless, portrait and image rights have certain added value: due to their status as a personality right that ensures a core of legal protection that cannot be easily contracted away; and due to the fact that these rights can be applied beyond individual pieces of data to the more holistic digital persona on OSNs.

After having conducted this more theoretic legal analysis of copyright and portrait rights on content and digital persona on OSNs, several things remain to be done in the next version of this deliverable (D3.12). First, the research in this deliverable on portrait and image rights with regard to digital persona on OSNs often encountered certain boundaries in the applicability of these legal concepts. Several aspects of the general personality right (as deduced from Art. 8 ECHR) and other non-image rights derived from this general right, loomed large as sources and inspiration to deal with these shortcomings. In the next version of this deliverable we will look at whether such personality rights could be used to further

protect the inalienable core of private life of OSN users to supplement the image right protection.

Secondly, in order for the argument to hold that the Databait user interface offers an 'educated guess' of the digital portraits of OSN users, more work needs to be done in making links to the types of datamining practices that Facebook can reasonably be surmised to engage in, if we want to plausibly claim that what Databait offers is a visualization of the normally invisible parts of the digital persona on OSNs. More multi-partner work might need to be done within the USEMP project in order to make these links. This is also of importance for qualifying what it is that Databait does exactly. If these links are not made, Databait cannot claim to provide a "simulation" or a "mimicking" of the data derivation that happens on OSNs like Facebook, but would rather constitute what we could call "parallel profiling". In this context, it could be useful to list the different ways in which profiles and digital personae are created and used, in order to then consider whether these operations are protected under the legal regimes of personality rights (especially image rights), especially in the light of the criteria of recognisability and identification.

Thirdly, in the next version of this deliverable, we will also look closer at how the findings of this deliverable translate into legal requirements for the DataBait architecture. We will report on the exact wording of the IP clause to be included in the DLA based on the research performed in this deliverable and deliverable D3.7. We will also investigate whether the Data Licence Agreement should be expanded by including other types of licences for the use of copyrighted content on user-generated content or portrait rights on the user's digital persona that is generated by the DataBait tools themselves. In this way systematic legal research nourishes the construction and adaptation of the DataBait tools, which should, in turn, feed on these findings. As such they are part of Legal Protection by Design as a reiterative process.

Annex 1 – The Social Ontology of Digital Personae on Facebook

An encompassing view of the ways in which the construction and commodification of the user's digital persona becomes enabled in online networked technologies, can be obtained when turning to the affordances provided by the interfaces that Facebook offers to advertisers.[85] Through these interfaces users become socially reassembled according to series of fundamental relational categories within network technologies. We can use a broadened conception of the notion of social ontology in order to understand these processes.[86] These categories are themselves made possible by the different channels of information flow within this technological infrastructure. We can distinguish the following **five modes of data capture**[87] and their correlated objectification into some of the ***basic concepts of the commodity ontology*** of online social networks[88]:

- **Registration data & page content** are basically data obtained by the ways of user engages in self-categorization either through the processes of joining the OSN, or the data disclosed on the pages of the user or others.[89] These data have an important self-referential identity character, which they share with the data entered for characterizing an event on Facebook. In the advertisement interface, registration and page content data these encompass most of the data categories for targeting users. Many of them include classical ***demographics*** like age, gender, education, languages, workplaces, relationship status, but they also include the ***specific interests*** indicated by the user.
- **Incidental data** capture information about a user through the behavior of other users. This relates primarily to the direct actions that the Facebook platform performs like tagging, posting, etc. In advertisement however incidental data plays a role on a different level through the "***connections***" category, especially by enabling the targeting of "friends of connections". This is a kind of social network analysis by which data about someone can be derived through their degrees of connectedness to others.
- **Traffic data** are basically meta-data not about the content of online behavior but which are often necessary for the carrying out of these behaviors.[90] On Facebook

[85] Another peak at the nature of this digital personae can be obtained by performing data access requests, either through a legal access request or through the "download my data" tool (https://www.facebook.com/help/405183566203254/).

[86] The term 'social ontology' was foundational in the transition to the social semantic web. For an account of the evolution of social ontologies, see: (Weber, 2008). We will here use the term in a broader sense.

[87] Some of these data categories overlap with the 6 types of data used in online social networks as distinguished by (Schneier 2010): service data, disclosed data, entrusted data, incidental data, behavioral data and derived data. Whereas the user actively discloses the first three types of data, this is not the case with the latter three types of data. See: https://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html

[88] This section is based on research in the EMSOC project (Heyman & van Dijk, 2013).

[89] This correlate with what Schneier calls service data and disclosed data.

[90] The e-privacy Directive 2002/58/EC provides the following exemplary list: "data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or

these traffic data include both the **technical/logging data** about the type of computer, type of operating software, type of browser of the user and more **browsing behavioral data** made possible by all kinds of online identifiers like cookies, session trackers, IP addresses, or through Facebook's single sign-on. This is a standard basis for web advertisement and plays a crucial role in Google's Analytics program. For advertisements on Facebook these data are relevant in the category ***location*** which can be determined on the basis of IP address[91], but also as one of the "broad categories" pertaining to what we can call the ***traffic medium*** used, which enables Facebook to extend to the mobile market and fine-tune the "placement" of its ads.

- **Interaction data** play an important role in OSNs. They include most of the social actions a user can perform on a networking platform.[92] For advertisement purposes they play a crucial role in the category of "interest targeting". These interests are taken from several indicators. The most significant action is the crucial function of ***liking*** that has become afforded through the design of the like button for direct preference indication and its plug-ins on other sites. Also very important is the ***subscription*** to applications that plug into Facebook and, as we have seen above, can render stories about the user through their underlying web semantics. Furthermore ***membership*** of groups or events is also interpreted as an indicator for interest.[93]
- **Inferred data** are data about a user derived from all these previous data types of the users and of other users obtained through data mining techniques in order to learn new information about people. We have become acquainted with these techniques in the discussion about profiling in this article. These data play several roles in the advertising interface. Firstly, Facebook offers a few pre-mined profiles included in the "***broad interests categories***" which especially relate to one's "family status". Secondly, when advertisers have selected certain likes and interests as targets Facebook automatically offers "suggested likes and interests". These are "the terms that are most common among the people your targeting criteria already includes."[94] These ***conjectured interests*** are thus likely derived through clustering methods or association rules, in order to aggregate group profiles with shared features. Lastly, we could probably also include Facebook "topic targeting" under inferred data.[95] Certain interest keywords include overlapping precise interests. These terms can be called ***topical interests***.

---

terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network."(recital 15)

[91] It could also be argued that the category of location is actually inferred data, since these data have to be derived from IP addresses which themselves do not yet directly indicate location. Furthermore, user location can also be obtained on the basis of self-categorization by the user.

[92] This correlate with what Schneier calls behavioral data.

[93] "Interest targeting helps advertisers target people based on information they've added to their timeline. This considers information such as the Pages they like, apps they use" and groups to which they belong, or "may be drawn from their listed interests, activities, education and job titles". This function thus also makes use of registration and profile data. https://www.facebook.com/help/www/453530464730606/

[94] https://www.facebook.com/help/www/453530464730606/

[95] https://developers.facebook.com/docs/reference/ads-api/topic-targeting/

Facebook is likely to store registration data, user generated content, incidental data, behavioral data and interaction data separately in different databases (or log files), in different schemas and tables.[96] On this basis different access permissions can also be set, which allows more fine-grained access control for different applications. Nevertheless, within these databases cross-references are inserted that link the data about a certain user in different databases together. Users can also be referred to via a unique identification number across all the different Facebook databases (Bronson et al. 2013). Thus, in spite of this physical storage dispersion of these different data types, due to these interlinkages they can thus functionally be considered together as a digital persona.

[96] With regard to inferred data, the number of attributes that can be linked to someone is virtually limitless. Yahoo for instance maintains millions of features for each user profile in its datasets, most of them as binary yes-no features indicating user interests, sizing to 1K per user. (see: http://www.slideshare.net/anmolbhasin/recommender-systems-the-art-and-science-of-matching-items-to-users-a-linkedin-open-data-talk-by-deepak-agarwal-from-yahoo-research). Facebook probably has even more features per user.

References

Article 29 Working Party. 2009. “Opinion 5-2009 on Online Social Networking.” Brussels.

———. 2011. “Opinion 15-2011 on the Definition of Consent.” Brussels.

———. 2014a. “Opinion 05-2014 on Anonymisation Techniques.” Brussels.

———. 2014b. “Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC.” Brussels.

Bertrand, A. 1999. *Droit à La Vie Priveé et Droit à L’image*. Paris: Litec.

Beverley-Smith, H. 2008. *The Commercial Appropriation of Personality*. Vol. 4. Cambridge University Press.

Bronson, N., Z. Amsden, G. Cabrera, P. Chakka, P. Dimov, H. Ding, J. Ferris, et al. 2013. “TAO: Facebook’s Distributed Data Store for the Social Graph.” In USENIX Annual Technical Conference. San Jose.

Brüggemeier, G., A. Colombi Ciacchi, and P. O’Callaghan, eds. 2010. *Personality Rights in European Tort Law*. The Common Core of European Private Law. Cambridge, UK ; New York: Cambridge University Press.

Bygrave, L. A., & Schartum, D. W. (2009). Consent, proportionality and collective power. In *Reinventing Data Protection?* (pp. 157-173). Springer Netherlands.Clarke, R. 1994. “The Digital Persona and Its Application to Data Surveillance.” *The Information Society* 10.

Curren, L., and J. Kaye. 2010. “Revoking Consent: A ‘blind Spot’ in Data Protection Law?” *Computer Law & Security Review* 26 (3): 273–83.

De Hert, P., and R. Saelens. 2009. "Het recht op afbeelding." *Tijdschrift voor Privaatrecht* 2: 867-917.

Dierickx, L. 2005. *Het Recht Op Afbeelding*. Antwerp-Oxford: Intersentia.

Heyman, R., and N. Van Dijk. 2013. "Who can Afford Users as Targets? Interfaces, Transparency and the Commodification of Relations in Online Social Networks". Report No. D3.3.1. EMSOC Project.

Hildebrandt, M., and N. Van Dijk. 2012. “Customer Profiles: The Invisible Hand of the Internet.” In *Databases - The Promises of ICT, the Hunger for Information, and Digital Autonomy*, edited by M. Schuijff & M. Besters Munnichs, G., 62–71. Rathenau Instituut.

Kosinski, M., D. Stillwell, and T. Graepel. 2013. “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior.” *PNAS* 110: 5802–5.

Kramer, A.D.I., J.E. Guillory, and J.T. Hancock. 2014. “Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks.” *PNAS* 111 (29): 10779.

Pinckaers, J.C.S. 1996. *From Privacy toward a New Intellectual Property Right in Persona*. Information Law Series 5. The Hague: Kluwer.

———. 2009. “Het Object van Bescherming: Van Portret Naar Persona.” In *Commercieel Portretrecht*, edited by D.J.G. Visser, 31–40. Amstelveen: deLex.

Roosendaal, A. 2013. *Digital Personae and Profiles in Law: Protecting Individuals’ Rights in Online Contexts*. Oisterwijk: Wolf Legal Publishers.

Schneier, Bruce. 2010. “A Taxonomy of Social Networking Data.” *IEEE Security and Privacy* 8: 88.

Solove, D.J. 2004. *The Digital Person. Technology and Privacy in the Information Age*. New York: New York University Press.

Synodinou, T. 2014. “Image Right and Copyright Law in Europe: Divergences and Convergences.” *Laws* 3 (2): 181–207.

Van Dijk, N. 2009. “The Legal Status of Profiles.” In *Intelligent Environments 2009*, edited by V. Callaghan, A. Kameas, A. Reyes, D. Royo, and M. Weber, 510–16. Ambient Intelligence and Smart Environments 2. Amsterdam: IOS Press.

Van der Sloot, B. 2015. "Privacy as Personality Right: Why the ECtHR’s Focus on Ulterior Interests Might Prove Indispensable in the Age of “Big Data”." 31(80). *Utrecht Journal of International and European Law* 25-50.

Vickery, G. and S. Wunch-Vincent. 2007. "Participative web and user-created content: Web 2.0 and wikis and social networking". Paris: OECD.

Voorhoof, D. 2009. “Commercieel Portretrecht in België.” In *Commercieel Portretrecht*, edited by D.J.G. Visser, 145–66. Amstelveen: deLex

Weber, N. 2008. “The Evolution of Social Ontologies.” Proceedings of the 3rd EC-TEL 2008 PROLEARN Doctoral Consortium, held at the European Conference on Technology Enhanced Learning, Maastricht, The Netherlands, 17-07-2008