



D3.12

Copyright and Rights in Digital Personae in Online Social Networks

v 0.7 / 2016-11-01

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

This document presents an analysis of the copyrights involved in content and digital persona on Online Social Networks (OSNs). It also investigates to what extent rights in (digital) personae 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.



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	Alexandru Ginsca (CEA) Andreas Drakos (Velti)
Version	0.7
Status	Final
Dissemination level	PU: Public
Due date	30 September 2016
Delivery date	1 November 2016
Version	Changes

0.1	Initial Release, Niels van Dijk (iCIS)
0.2	Adjustments based on internal discussion Niels van Dijk, Katja de Vries, Sari Depreeuw and Mireille Hildebrandt (iCIS)
0.3	Adjustments and additions by Katja de Vries (iCIS)
0.4	Adjustments after internal review by Alexandru Ginsca (CEA)
0.5	Adjustments after internal review by Andreas Drakos (Velti)
0.6	Adjustments Niels van Dijk (iCIS)
0.7	Adjustments Katja de Vries (iCIS)

Table of Contents

1. Introduction	4
2. Copyright	5
2.1. Copyright in individual pieces of (user generated or third party) content - and their licenses	5
2.2. Copyright in User Profiles and Digital Persona on OSNs	11
3. Rights in Persona	16
3.1. Rights in Digital Personae on OSNs	16
3.2. What is the Added Value? Comparing rights in persona to data protection rights	21
4. Conclusion	32
Annex 1 – The Social Ontology of Digital Personae on Facebook	34
References	37

1.Introduction

In this deliverable we present an analysis of the copyrights and rights in persona involved in the user profiles on Online Social Networks (OSNs). In D3.11 we discussed the intellectual property rights which can be mobilized by OSNs to fend off transparency efforts. In this deliverable we discuss the other side of the coin: the rights of OSN users in their profiles. In this way we want to explore what other legal means of empowerment a user might have with regard to her data on OSNs apart from the 'usual suspects' such as data protection and privacy rights (see D3.10). One of the innovative aspects of this deliverable is that we do not merely focus 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 rights in persona like 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.

2. Copyright

In this section, we 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. OSN users might hold copyrights over the user generated content they post on their profiles. Third parties whose copyright protected content (re-posting of news articles, music videos, art works, etc.) is placed on the profiles of OSN users also might hold copyrights. Can these copyrights of users and third party authors interfere with this content being used in profiling processes? Users normally give far-reaching copyright licenses to OSNs (such as Facebook). As long as these licenses hold up in court, OSNs cannot be hindered in their profiling processes by the copyrights of their users. Third party content, however, poses more complex issues. Can this content be used for profiling processes without any license? This is a challenging question for OSNs. According to the dual USEMP objectives of user empowerment and tool compliance, the investigation here will also turn towards the content used by the DataBait tools themselves. Like for OSNs, it is studied how the reproduction of third party content for profiling purposes needs to be handled.

After having looked at copyrights in individual pieces of content, 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. Here we will especially turn to an analysis of database rights.

2.1. Copyright in individual pieces of (user generated or third party) content - and their licenses.

2.1.1. Copyrights over individual pieces of posted content held by OSN users and/or third parties.

Almost any form of profiling requires that copies are made of the data that are analysed. This, obviously, goes both for the profiling that large OSNs, such as Facebook, perform on user data, as well as the “profiling-for-the-sake-of-transparency” done by DataBait.

Let us begin by taking a closer look at DataBait. In order to allow DataBait’s “profiling-function” to work (i.e. showing the user what the DataBait algorithms can extract from their OSN data) copies need to be made of the user’s OSN data – both during the development and the operation of DataBait. Some of these data (e.g. photos, textual posts, videos) are likely to be copyright protected content. Making copies (reproductions) of copyright protected content without the permission of the author or another right-holder is a restricted act according to copyright law. The author of copyright protected content, which is reproduced by DataBait, can either be the OSN user (in this case we speak of “user generated content”: e.g., the OSN user posting her own holiday pictures on her profile) or a third party (e.g., the OSN user re-posting a music video of her favourite musician on her profile). As discussed in

D3.11 (section 2.4.2) such copying for the sake of the profiling process of DataBait could possibly¹ be qualified under the copyright exception for temporary acts of reproduction (art. 5(1) of Directive 2001/29, the so-called “Copyright in the Information Society” or “InfoSoc” Directive). Moreover, as long as DataBait has a scientific purpose (which was the case during the whole USEMP project) the copyright exception for scientific research (art. 5(3)(a) InfoSoc Directive) applies.² As such the risk of infringing on copyrights on individual content during the duration of the USEMP project is extremely low³. However, given that the USEMP consortium is exploring possibilities to maintain a specific post-USEMP version of DataBait online after the project has ended, and that the purpose of this version would possibly be non-scientific (though still strictly non-profit), it is necessary to explore how DataBait’s processes could function if no copyright exception were to apply. In as far as the copyright

The copies made for DataBait’s profiling process are unlikely to infringe on copyrights of individual pieces of content posted on an OSN profile because (1) there are exceptions for temporary acts of reproduction and for scientific research, and because (2) each DataBait user signs a copyright clause licensing USEMP to make copies for the purpose of profiling.

protected content copied by DataBait is user generated content, there is no copyright infringement because each DataBait user gives a copyright license (limited to copies which are necessary for DataBait’s profiling process⁴) to DataBait in Article (C) of the *DataBait Data*

¹ See D3.11, section 2.4.2. We argue that the exception for temporary technical copies should be applicable to DataBait. However, there is no sufficient case law, and thus legal uncertainty, as to whether the relevant Courts would find this exception applicable to DataBait.

² See D3.11, section 2.4.2, for a discussion of the applicability of the existing copyright exceptions for scientific research and for temporary technical copies, and of the proposed exception for text and data mining (TDM). There we concluded that the copies made for the sake of DataBait’s profiling process fall under the scientific exception (at least during the duration of the USEMP project; if DataBait is exploited for a non-scientific purpose after the end of the project, this would obviously change) reproductions made by DataBait), and maybe also under the exception for temporary copies. The proposed TDM exception is currently still in the stage of being a mere legal proposal and does consequently not apply. However, if the TDM exception would become actual law it could be very relevant for DataBait’s profiling process (it would depend on the exact formulation of the exception – something which is currently still contested).

³ The only (very unlikely) possibility would be if no copyright exception were to apply, i.e. a judge decides (contrary to what seems likely to us) that the exception for temporary acts of reproduction does not apply to DataBait and the scientific exception does not apply (this would surprise us as well – however because of our limited resources we could only do a global check; we were not able to check if and how the scientific exception is transposed in the national laws of each and every individual EU member state; so we cannot guarantee that each member state has transposed the exception or transpose it in such a way that it covers DataBait). The processing of user generated content created by DataBait users would still be covered by the license each user grants to DataBait in article (C) of the Data License Agreement (DLA). However, the reproduction (for DataBait’s profiling purposes) of third-party content posted, without the consent of the right-holder, on the profile of the OSN user, could in such scenario potentially be qualified as an infringement.

⁴ This specificity makes the copyright license in DataBait’s DLA very different from the broad, « blank check » type of copyright licence users give to large OSNs like Facebook. We discuss the Facebook copyright license later in this section.

Licensing Agreement (“DLA”, see D3.10 and D3.11). However, what about the third party content? The DataBait user cannot license that which is not hers to give. This would entail that, under the hypothesis that no copyright exception applies, it is up to the person(s) or entity running DataBait after the end of the USEMP project to seek the consent of the rights holder of the used third-party content. Acquiring the consent of the individual rights holders of third parties is in practice an unrealistic task: this would imply asking every author (or other right holder) of re-posted articles, posts, tweets, photos, music videos, etc. to license DataBait to make a copy of this content in order to infer additional information about the OSN user. The complexity of such an endeavour would be endless: not only the process of identifying and contacting each right holder, but also the serious possibility that many of these right holders will deny a permission for any reproduction unless a licensing fee is paid.

What about the third party content (re-posted articles, posts, tweets, photos, music videos, etc.) on an OSN profile? The DataBait user cannot license that which is not hers to give.

A DataBait user signs up for this transparency application precisely because she *wants* to enable DataBait to analyse her user profiles – to look for the inferable in her data. In the DLA she licenses DataBait to copy her data for the profiling process; a process which, most likely, is also covered by applicable exceptions for temporary acts of reproduction and use for scientific research. Even if we completely abstract from the legal context, it would be very paradoxical if a DataBait user would want to try to prevent DataBait’s profiling by, for example, mobilizing IP-rights. However, what about other right-holders? Are there right-holders which might have stakes in preventing DataBait’s transparency profiling? In Article 2.1 of the *Facebook Statement of Rights and Responsibilities*⁵ (version of January 30, 2015) every Facebook user gives a non-exclusive, transferable, sub-licensable license to Facebook. This means that a Facebook user continues to be the copyright holder over her own IP content and that she can license others next to Facebook (the license is non-exclusive). Facebook acquires a licence to use the user’s content but does not become the sole owner of the rights to the posted content. Considering that the general IP clause in Facebook’s general terms and conditions provides a non-exclusive licence, USEMP does not need Facebook’s consent to process protected content from users (or third parties). A licence from the Facebook user to USEMP is then sufficient, Facebook cannot prohibit the creation of the DataBait tools on the ground that its prior consent is required (in addition to its users’).

The context to the profiling to which the user is “subjected” by DataBait differs from the situation of the profiling performed by an OSN. A user does not sign up for Facebook out of desire to be commercially profiled; it is something that “comes with the package”. Yes, the user might *want* the profiling in as far as it improves the delivered service (e.g. an uncluttered newsfeeds only containing information that the user is interested in) but it probably will be hard to find a user who signs up to Facebook because of the personalized ads. So, it is very

⁵ Online available at: <https://www.facebook.com/legal/terms%20>

well feasible that a user would like to oppose being profiled. Can she mobilize IPRs against the profiling she is subjected to by the OSN? At first sight this is not very likely given the aforementioned non-exclusive, transferable, sub-licensable license which each user gives to Facebook when signing up for the service. However, it should be noted that it is far from certain that the legal validity of this copyright clause in Facebook's terms would hold up in court. The legal validity of such far-reaching licenses 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) could be challenged from the perspective of consumer and contract law (Wauters e.a, 2014). Also, Art. 7(4) of the new General Data Protection Regulation 2016/679 could pose problems for Facebook's IP license:

“When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract”. (italics ours)

It could be argued that making the use of Facebook's service conditional on a far-reaching IP license that allows for the processing of personal data that is not necessary⁶ for the performance of the core service makes it questionable if the consent for Facebook's data processing is freely given.

When broad and unspecific IP licenses are legally invalid, profilers would be required to reconsider the exact form of an IP license for reproduction, extraction and re-utilization for profiling purposes.

So, when broad and unspecific IP licenses are legally invalid, profilers would be required to reconsider the exact form of an IP license for reproduction, extraction and re-utilization for profiling purposes. In the case of a commercial profiler the type of exploitation might become relevant. Under many European copyright laws, copyright licenses with the author have to meet certain requirements (as a matter of substance or for evidence purposes) such as specificity with regard to the intended uses. The ratio for such specific copyright contract rules is generally to offer more protection to the author, who is considered the weak party in a negotiation with a professional party that will commercially exploit the work. The fact that OSN providers exploit IP-protected content in a way which differs from “traditional” exploiters (they exploit the content on an aggregated level; there is no traditional “publication” of reproduced content such as in the form of a pirated copy of a movie or a book⁷) and offer

⁶ The rationale behind Art. 7(4) seems to be that a service should preferably not be offered in such a way that it *only* can be acquired in exchange for personal data. Consent is only freely given if there is some choice, for example the choice between a service in exchange for a monetary payment or in exchange for data; or the choice to use a truly free service (no exchange). Recital 43 seems to make this point: «Consent is presumed not to be freely given if [...] the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance».

⁷ Commercial profilers (such as large OSNs like Facebook, LinkedIn, Google Plus, etc.) exploit “data” and “content” at an aggregated level (and not at the level of the individual content or based in the

their OSN to the user/author without requesting a monetary fee (though requesting a counter-performance by providing personal data), might shift the equation in favour of the OSN provider, resulting in a lesser protection for the user/author. This, however, goes beyond the scope of this report and is something that would need additional research.

Moreover, independent of the question whether licenses like Facebook's "non-exclusive, transferable, sub-licensable license" would hold up in court, third-party content can give head-aches to commercial profilers such as Facebook and other large-scale OSNs. After all, notwithstanding how far-reaching the Facebook copyright license is, it cannot cover third party content: as we said earlier, a user cannot give a license over that which is not hers to give.

Third-party content can give head-aches to commercial profilers such as Facebook and other large-scale OSNs. After all, notwithstanding how far-reaching the Facebook copyright license is, it cannot cover third party content.

2.1.2. Copyright exceptions for Text- and Datamining

As clarified in the previous section, currently both scientific, non-profit profilers as well as commercial profilers have a complex, rather unwelcoming, legal landscape facing them as regards copyright protection of content used as input for profiling processes. No wonder then that the recent proposal⁸ to revise the Infosoc Directive 2001/29/EC will include some kind of Text and DataMining (TDM) exception⁹ to make the life of profilers easier. In the proposal the exception only covers non-commercial profiling, though there are (understandably – given the interests!) strong lobby groups to make the exception also applicable to commercial profiling.

'originality' of such work). Arguably, such exploiters use digital content, including copyright protected content, but their model is evidently different from the exploitation model of, let's say, a film distributor or music label. Thus, the exploitation model of commercial profilers covers copyright protected content but in a sense it is not founded on the original character of the creations. They are interested in the copyright works as "data" or "driving data traffic". For example, a picture made by an OSN user of her breakfast cereal is not appreciated by the OSN for its "originality", nor exploited individually by the OSN. However, such picture has value for the OSN on an aggregated level and as an attractor of data traffic for targeting and profiling practices (e.g. the likes and the comments of the friends of the OSN user). If a legislator considers taking a normative stance towards the notions of "reproduction" (copyright protection), it will also have to consider whether protected elements are reproduced when a work it is not exploited for its originality, when it is not used as a work "as such" and has little value as a copyright work.

⁸ Brussels, 14.9.2016 COM(2016) 593 final 2016/0280 (COD). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market. Online available : <http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-593-EN-F1-1.PDF>

⁹ See also deliverable 3.11 on this exception.

In this section we will not enter into this debate but only provide a short exploration of how profiling (“TDM”) can be made easier for researchers within the EU. We argue that a simplification can be achieved in three ways (Hargreaves e.a., 2014).

How can profiling (“TDM”) be made easier for researchers within the EU? Firstly, proprietors of copyrights and sui generis database rights could grant liberal licenses to researchers. Secondly, the legislator could create an exception for TDM for research purposes. Finally, the courts and/or the legislator could give a restrictive interpretation to the notion of "reproduction", so that the copies made for TDM in a non-commercial context fall outside the scope of copyright and database law.

The first way can be achieved by the proprietors of copyrights and sui generis database rights: the owners of these exclusive rights could grant liberal licenses (allowing TDM for research purposes). This would be helpful in the development stage of research projects as USEMP, where databases are used to train algorithms. The second way would be through a change in copyright legislation, such as the aforementioned one in the proposed revised InfoSoc Directive, namely by creating an exception for TDM for research purposes. If the legislator was to create a copyright exception for TDM for scientific purposes, this would be important for research projects like USEMP. The third way would be up to the courts and/or the legislator: by making the notion of "reproduction" more restrictive (so that the copies made for TDM fall outside the scope of copyright and database law).

"The reproduction right in copyright law, as the right of extraction under the database regime, has traditionally received a broad interpretation encompassing any direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part of his/her work. After years of expansive interpretation, it seems timely to ask whether this broad interpretation of the reproduction/extraction right should be reconsidered. Instead of a functional approach to the reproduction/extraction right where all acts of reproduction or extraction that are technically possible fall within the scope of the owner's exclusive right, the legislator could take a normative approach and only recognise protection for acts of reproduction or extraction that actually entail an act of 'expressive' exploitation. Is TDM a form of copyright or database exploitation that should be under the control of the rights owner? Is TDM (in all its forms) an act of reproduction (and eventually of communication to the public) that affects the interests of the rights owner?" (Hargreaves, 2014, p. 53)¹⁰

Would such a normative interpretation of the word "reproduction" mean that the commercial exploitation of data would also fall outside the scope of copyright protection? And that OSNs like Facebook, Google plus and LinkedIn could mine user and third party data without needing a licence? This depends on the normative interpretation, but most likely not:

"[The] normative approach to the definition of the right of reproduction/extraction [could be]: if an act of reproduction of a work gives rise to no exploitation of that work, then this act of reproduction should not fall under the control of the rights owner."
(Hargreaves, 2014, p. 53)

The legislator could take the normative stance that the fact that a profiler *exploits* – in whatever way – copyright protected works (even as part of aggregated data) would entail that the copies made for the mining/profiling are still considered as “reproduction” in the sense of copyright law. The legislator could also differentiate between different types of exploitation. While the normative stance is not very common, differentiating between types of exploitation is useful when drafting licensing conditions as it offers an alternative to the aforementioned undesirable, and possibly even legally invalid, broad and all-encompassing copyright licenses like the one included in Facebooks user terms.

2.2. Copyright in User Profiles and Digital Persona on OSNs

The next question is whether profiles of OSN users could themselves merit legal protection as a whole. Here we get to a more speculative inquiry into two possible legal routes that could serve to empower users. In the next chapter (chapter 3) we will deal with the question of “rights in persona” (that is, rights to images, name and voice) in profiles. In this section we will explore the question of copyrights in profiles: Can user profiles themselves qualify as copyright protected works? And, if so, can OSN users claim authorship in them, or could OSN providers do so?

***Can user profiles themselves qualify as copyright protected works?
And, if so, can OSN users claim authorship in them, or could OSN providers do so?***

User Profiles & Digital persona

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".¹¹ 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".¹² This definition emphasizes the user has provided the data with regard to personal details or current situation, which are visible on someone's personal page on an OSN. She 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.¹³ Data about current situation are often provided in the processes of actual usage of the OSN by writing posts, or uploading content, etc.¹⁴ 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 algorithms.

For this reason a distinction should be made in the analysis between the visible **user profiles**, and 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.

A distinction should be made in the analysis between the visible user profiles, and the larger digital personae that are pieced together by OSNs on the basis of different data sources

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

¹¹ Oxford Dictionary.

¹² *Ibid.*

¹³ Few data will be protected under copyright at that point (except perhaps for a tag line or a personal description).

¹⁴ 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".

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).

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 models: such ‘user profile’ 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. The visible user profile is just a subset of this larger digital persona.

Copyright

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, we will answer two questions. First, can the profile be considered a “collection” or a database?¹⁵ Second, is the profile an original creation by the user?¹⁶

1. Can user profiles and digital persona on OSNs be qualified as **databases** that are protected by intellectual rights? In Europe this subject matter is covered by the Database Directive.¹⁷ The object of protection - a “database” - is here defined 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" (Article 1(2)).

Application to OSN user profiles and digital persona:

- ‘a collection of works, data or other materials’:

Yes, a collection of different data (in the sense distinguished in Annex I),

- ‘independent’:

Yes, the different data are independent of each other due to the way they are ordered as distinct entries in the profile format.¹⁸

- ‘arranged in a systematic or methodical way’:

Yes, the ordering of data that make up the collection according to the data types or categories (timeline, about, friends, photos, etc.) of the profile is systematic.

¹⁵ 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. In this deliverable, we will only be discussing issues of copyright on databases and not of the *sui generis* database rights.

¹⁶ (Van Dijk 2009).

¹⁷ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

¹⁸ 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.

- *'individually accessible by electronic or other means':*

Yes, the OSN can electronically access all the data. This is sufficient.

2. Is the way the data are selected or arranged **original** in the sense of copyright law? The originality criterion for copyright protection is defined as follows:

"databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation" (article 3.1 Directive 96/9/EC).

This implies the user has had the possibility to make choices during the creation process and that the way these creative possibilities have been used constitute sufficient personal contribution to the shaping of the profile.

Application to visible user profiles:

- *'arrangement'*

No. The design of the user interfaces on OSNs like Facebook and Twitter offer the user a preset format for data entry that s/he fills in. This does not, or barely, leaves the user any creative space for choosing the way these data are systematically and methodically ordered.

- *'selection'*

Yes. 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.). Large parts of the visible user profile have been selected 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.

- *'the author's own intellectual creation'*

Maybe. Does 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 the user's personality through her online actions. It could however be questioned how much creative activity can really be found in this.

Application to broader digital persona:

- *'arrangement'*

No. The OSN provider decides on the structure of this database format.

- *'selection'*

Very limited. Although 'registration data' and 'disclosed data' are selected by the user, this is not the case for the other data types (see Annex I). Other OSN users ("friends") select the 'incidental data'. The OSN creates the 'behavioral data' and 'inferred data' about the user. It further provides the preset entry format for the types of relational actions ('interaction data') the user can take (membership, commenting, tagging, liking, checking in).

- *'the author's own intellectual creation'*

See above

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. 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. OSN providers can more likely claim copyright in these more encompassing data arrangement that constitutes the user's digital persona on OSNs. Furthermore, 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.

***Do digital personae constitute copyrightable works as databases?
Even if this question is answered positively, users could only exert
rights on a very small part of their digital persona, namely the visible
parts of the user profile and not on the larger digital persona.***

***Furthermore, copyright in databases merely protects the form in
which the data are combined and in this sense only offers some
protection when data re-combinations create derivate works of the
original profile, or affect its integrity.***

3. Rights in Persona

We will now turn away from intellectual rights for purposes of user empowerment and direct our attention to a different legal field. We will explore whether what we will call “rights in persona” like rights to images, name and voice, can be used as a ‘trump’ for OSN users over some of the intellectual rights of OSNs. Due to their status as personality rights, these rights ensure that there is a core of legal protection that cannot be contracted away.

By turning to rights in persona 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. 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 D3.10, the user might also exert certain rights in her digital personae. The field of rights in persona 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 rights in persona like image 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 rights in persona offer added protection for the data subject compared to the regime for the protection of personal data.

3.1. Rights in Digital Personae on OSNs

Can users claim any personality rights in profiles or digital persona on OSNs? In this section we will approach this question by exploring the concept of “rights in persona”, which is a bundle of right including portrait rights, image rights, rights in name, and rights in voice. These rights protect a series of characteristics that allow to identify someone, by granting a person the right to object to their (commercial) usage. In order to situate and understand the concept of “rights in persona” and how it used in this deliverable, we need to first clarify the tools of analysis by making a conceptual distinction between “portrait rights”, “image rights” and a general “personality right”.

A **‘portrait right’** is a very specific legal term in copyright legislation of some EU member states like the Netherlands and Belgium (*“portretrecht”*)¹⁹ and Germany (Rechte an Bildnissen” or “Porträts”)²⁰. Due to their incorporation in copyright law, portrait rights are generally only evocable in case the relevant portrait is a copyrightable work.²¹ These rights

¹⁹ Article 20-21 of the Dutch *Auteurswet*; article 10 Belgian *Auteurswet*.

²⁰ Article 22 of the German *Kunsturhebergesetz*.

²¹ 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.

function as a restriction on the exercise of copyright by its right holder on an image in which the portrayed person is depicted.

Image rights do not have this limitation to copyright. In the Anglo-Saxon world it is called the “*right to one’s image and likeness*”, in French it is called a “*droit à l’image*”, and in German a “*Recht am eigenen Bild*”. It relates to the set of visible characteristics and acts of an individual that allow her identification. They are broader in scope than portrait rights and can be considered a superset of these.

Image rights are a **specific personality right** next to other personality rights like right to name or other unequivocal identity aspects. They are based on the **general personality right** and the **right to private life**, which can be derived from Art. 8 of the European Convention of Human Rights, or national constitutional rights such as Art. 1 and 2.1 of the German Federal Constitution, or article 9 of the French Civil Code.

The general right of personality is an absolute, comprehensive right to respect for and development of personality.

Image Rights in Europe

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 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. 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.” (ECHR, 15 January 2009, 1234/05, §40).

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. 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.

1. Protected subject matter: from images to persona. 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.²² Nevertheless, these representations of a person 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, 129-133; Dierickx 2005, 66-74) that involves several criteria.

1. The portrayed person does not need to be identifiable from the perspective of strangers, but could also be identified from the perspective of persons who know her.
2. Direct or immediate identification is not necessary, but closer investigation and comparison is also possible. Additional circumstances than the portrait (name, family, clothing, surroundings, origin, distribution of non-anonymized version of the image) can play a role in this identification. 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 like haircut, color of hair, body silhouette, posture, clothing style.²³ The test is thus 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 similar protection as portraits in the case-law of several EU member states, many of these as separate specific personality rights. The criterion of recognizability and identifiability are also central here.²⁴ For this reason, it has been argued for shifting the attention from the term portrait, which has more limited applicability, to that of **rights in persona** as the object of legal protection (Pinckaers 1996). This is a bundle of (personality) rights that include this whole legally protected range of distinctive elements or indicia by which a natural person can be identified. In this deliverable we will adopt this concept of rights in persona for our analysis, since its scope provides the closest fit with our object of analysis: digital persona on OSNs.

Application to OSN user profiles and digital persona:

- *the technical medium is irrelevant*

The technical way the portrait is made is largely irrelevant (or voice is captured) for the application of right in persona and could thus apply to digital media and representations. Image rights however only apply to representations that can be mainly visually recognized. Whereas the visible OSN user profiles are indeed composed of some visual elements like photos, videos or posts, the more encompassing data model making up the digital persona 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

²² 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.

²³ HR 2 may 2003, NJ 204, 80 (Breekijzer); V.zr. Rb. Breda 24 June 2005, AMI 2005-5, nr. 14 (Gouden Gids & Katja Schuurman vs. Yellow Bear).

²⁴ 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) or the one to whom it refers, is based upon or inspired by. 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), (Brüggemeier, Colombi Ciacchi, and O'Callaghan 2010, pp 206 ff.)

image data. When we however broaden the scope of analysis to rights in persona, other non-visual elements also have to be taken into account.

- *identification & recognition*

Yes. The important test behind rights in persona was whether the represented person could be identified by (a combination of) distinctive traits, 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. Identification is 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.²⁵

2. Scope of protection: Right to prohibit

In most jurisdictions, the right holder of rights in persona is granted a series of actions. The most important is the right to prohibit the *publication* of the representation without the consent of the person represented. This ‘right to prohibit’ also 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.

Portrait rights only allow the right holder to prohibit the publication of the portrait and offer no protection against the making or reproduction of the portrait. The phase of making the portrait is here thus irrelevant, it is rather the moment of marketing the product that determines whether a legal action can be instituted (Pinckaers 1996, pp. 136-137).

Image rights, to the contrary, also include the right to prohibit the *making* of the portrait without consent of the portrayed person.²⁶ 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).²⁷ This focus on general commercial and non-commercial use of the image provides for quite a large scope of legal action.

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*

²⁵ 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 image rights can be applied by analogy. The user’s digital persona on OSNs could then be qualified as his or her digital portrait in the sense of the law.

²⁶ (Voorhoof 2009, p. 155), (Dierickx 2005, pp 85-86).

²⁷ 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).

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 to OSN user profiles:

- *publication*

This depends on the user's privacy settings. 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'.²⁸ In an Opinion on Online Social Networking, the Article 29 Working Party has determined 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 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.

Application to OSN digital persona:

- *publication*

²⁸ 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.

No. No one apart from the OSN itself has access to the broader data categories (inferred data, behavioral data) that make up the digital persona, not even the user herself. In this sense the digital portrait is never made public.

- *recording and conservation*

Yes. Image 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. 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.

- *commercial and non-commercial usage*

Yes. Facebook uses the digital personae of the user for commercial purposes for obtaining advertisement revenue. This usage is not related to the outgoing side of the portrait, the presentation of this personal information to the public, as is the case with classical portrait rights cases. It rather to the incoming side: the fact that the user receives advertisements based on her profile.²⁹

3.2. What is the Added Value? Comparing rights in persona 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 rights in persona an interesting option for user empowerment, especially in the context of the DataBait tools? In this section, we will first discuss the similarities between rights in persona and data protection law with regard to their protected subject matter and scope of protection. Afterwards we will discuss whether they add anything to the protection and guarantees offered by copyright and data protection law.

1. From the perspective of empowerment, it might be interesting to compare rights in persona 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).

²⁹ One form of usage that might be interesting in the OSN case is that of « provision », or « putting at the disposal of ». Facebook does not provide direct access to advertisers of the user's profile data, but rather lets the advertiser select the audience in terms of general categories after which Facebook itself places the ad at the address of those users who fit this group profile. The court of Brussels has determined that providing images of someone to a marketing agency for financial return is a form of usage in the sense of image rights. Rb Brussels 19 January 1999, A.R. 97/9254/A, discussed in (Dierickx 2005, p. 93).

A. In the section above we have mentioned that the definition of the protected subject matter of rights in persona – the persona indicia - depends on a test of *identification* (and recognition). The same is true for data protection law. Personal data are defined as

“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Article 4.1 of the General Data Protection Regulation 2016/279/EU).

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 for rights in persona.³⁰ The test of identification for each specific personality right (image, name, voice) might be more limited to a certain human sense (visual, auditory), than it is in data protection law, where the identification typically takes place through the use (or combination) of all kinds of identifying data. This contrast is reduced however, by using the combinatory bundle of rights in persona reduces and by the fact that data protection law does not specify the means through which the identification takes place. Nevertheless, a remaining difference might be the fact that identification in rights of persona is performed by humans (friends, strangers), whereas in data protection it can also be done by a computer.

The identifiability of a certain natural person by (a combination of) certain indices determines whether we can speak of the personal data of data protection and the representations of rights in persona.

Anonymization also plays a similar role in both legal regimes. Due to this test of identification, the application of rights in persona 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 (by the judge) may result in identifiability, which can also result from the combination with additional indirect circumstantial factors. Identifiability is also the main criterion for applicability of data protection law and may also 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,³¹ 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 it rather depends on the proceeding state of the art of the

³⁰ See also (Roosendaal 2013, p. 243) on this similarity between DP law and portrait rights.

³¹ Court of appeals Amsterdam, January 14, 1993, AMI 1993 (*former champion lightweight*), discussed in (Pinckaers 1996, pp. 131-132).

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

Pseudonymous data

In this context it also deserves mentioning that article 4.5 of the GDPR introduces the new notion of 'pseudonymisation' defined as:

“the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

While 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 personal data and anonymous data. It rather functionally deals with the risk and likelihood of identification of an individual. 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 pseudonymous, not anonymous. This concept might also be relevant for portrait or image rights.

of a previously anonymized piece of data and thus cancel out the effect of anonymization.³²

B. The second point of comparison between image rights and data protection law is the scope of protection: the *right to object* (or prohibit) and the possibility to withdraw consent. Article 21 of the General Data Protection Regulation grants the data subject the right to object at any time to the processing of data relating to her. This right 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 6(f) General Data Protection Regulation – GDPR).³³ Such interests can include quite different things ranging from broad societal benefits to more narrow economic interests.³⁴ These legitimate interests of the data

³² Recital 26 of the GDPR states that “To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”

³³ 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 on portrait rights 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), (Synodinou 2014, pp. 189-191).

³⁴ “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

controller have to be balanced against the “overriding” interests, rights and freedoms of the data subject, which they can only outweigh when they have a “compelling” character.

Rights in persona and data protection both offer the legal subject a right to object to the use of information that identifies her.

The objection by the data subject made in these circumstances has to be made “on grounds relating to his or her particular situation” of the processing of personal data (article 21.1 GDPR). Nevertheless, this standard is not required in case the personal data are or will be “processed for direct marketing purposes” by the data controller or by a third party to whom these data will be disclosed and by which they will be used (article 21.2 GDPR). This includes marketing for which profiling techniques have been used. Here the Regulation unconditionally states the data subject is offered the right to object to such disclosure and use at any time.

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.

Article 21 *Right to Object*

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Article 6 *Lawfulness of processing*

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (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;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (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;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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).

2. In the light of this comparison, we can thus proceed to ask what is the *added value* of the use and application of rights in persona for protection on OSNs in relation to data protection law? Three distinctions will be discussed:

A. Firstly, we have to explore whether the fact that rights in persona are **personality rights** offers advantages over rights derived from data protection law,³⁵ especially with regard to the role of *consent*. A personality right has an absolute, non-patrimonial, inalienable character (Dierickx 2005, p.2).

- The absolute character entails it offers legal protection against everyone (*erga omnes*) and for instance not just against the one who created the image.³⁶
- The non-patrimonial character entails that the image is not reducible to monetary valuation and that it does not belong to someone's patrimony.³⁷
- 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. 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.³⁸ Rights in persona can thus be of help when a user has unknowingly licensed away too much of her intellectual property rights. Moreover, one cannot consent to uses that did not exist and could not be foreseen at the time of signing.³⁹ This makes it impossible for a user to waive the exercise of her rights based on a clever legal contract with an OSN.

³⁵ 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).

³⁶ 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 6f GDPR.

³⁷ 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.

³⁸ Although such revocation may of course have consequences, since the user might have to compensate the OSN.

³⁹ 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.

Comparison to Copyright

Copyright law also provides a mix between moral rights that are inalienable and cannot be transferred away (the right to integrity and the right to paternity/attribution of the work) on the one hand, and economical exploitation rights (like 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 on the other hand. Moral rights limit what you can contract away and the ways in which a contract can be composed. One can for instance not allow a person or organization to deny that you are the author of a text. It is also 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

Data protection is a fundamental right,⁴⁰ but not a personality right.⁴¹ Consent plays an important role within this regime. The General Data Protection Regulation now explicitly acknowledges that *consent* can also be *revoked*.⁴²

“The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.” (Art. 7(3) of the GDPR)

This is similar to consent with regard to personality rights. This role of consent in data protection has to be qualified however. Consent (Art. 6(a) of GDPR) in data protection is never absolute: the proportionality of what the data subject consents to has to always be tested.⁴³ A data subject can for instance not give consent to processing of data that are not adequate or relevant, or which are excessive in relation to the purposes for which they are processed.⁴⁴ Furthermore and more importantly, consent is not a prerequisite 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 6 of the GDPR.⁴⁵ If another ground has been chosen, withdrawal of consent is thus an ineffective option.⁴⁶

⁴⁰ According to article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01).

⁴¹ Personality rights and fundamental rights differ in the following aspects (Senaev, 2008, nr. 431-432): 1) fundamental rights contain obligations of the State in relation to citizens (vertical relation) whereas personality rights contain obligations between citizens (horizontal relations); 2) fundamental rights belong to the European order, whereas personality rights often belong to internal national orders (of EU member states); 3) fundamental rights belong to public law, personality rights belong to private law.

⁴² Furthermore, the e-privacy directive that deals with location data and traffic (meta-) data relating to electronic communications, 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 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).

⁴³ However, see Bygrave & Scharf (2009), who find consent is not subject to a proportionality test.

⁴⁴ Article 5.1(c) GDPR.

⁴⁵ Consent is however 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).

⁴⁶ See (Curren and Kaye 2010).

Rights in persona do not have these types of limitation.⁴⁷ The fact that they are a personality right makes them an interesting complementary right to data protection rights. They guarantee an inalienable core of the intimate sphere that cannot be contracted away through user licensing. This core goes back to the fundamental right to privacy as protected in article 8 of the European Convention of Human Rights.

Rights in persona and data protection rights have different complementary cores - protection against the use of personal representations and good administration of personal data - that cannot be 'consented away'.

In this sense, the difference between both could be related to the difference between the core of the fundamental right to privacy and the core of the fundamental to data protection. The European Court of Human Rights determined that the right private life as enshrined in article 8 of the Convention “is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings”.⁴⁸ In the context of digital technologies, the European court of Justice has further specified that the core of this right protects against access to the content of electronic communications, whereas the core of the right to data protection is made up by principles of data processing.⁴⁹ This can be called a difference between privacy as an *opacity tool* for the citizen as a *freedom against outside intervention* (Gutwirth & De Hert) and data protection as a *tool for good administration* of personal data by the data controller (according to principles like fairness, lawfulness, transparency, purpose limitation, proportionality and accountability) and for data security (according to principles like integrity and confidentiality).

Right in persona like image rights are derived from this right to private life. In the context of representation technologies like photography, the ECHR has stated that:

“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 or her 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.”⁵⁰

In a broader sense we could say that the core of right in persona is the protection of representations of a person. The cores of both the fundamental rights to privacy and data protection cannot be contracted or consented away, but they relate to different things. This is a difference between how certain third actors can deal with someone’s data (that make up your digital persona), and what those data are about and how to control them.⁵¹

⁴⁷ 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.

⁴⁸ ECtHR, 7 February 2012, 40660/08 and 60641/08, von Hannover v. Germany (no. 2)

⁴⁹ ECJ, 8 April 2014, C-293/12, Digital Rights Ireland; ECJ, 6 October 2015, C-362/14, Schrems v Data Protection Commissioner (Safe Harbour).

⁵⁰ EHtCR, 15 January 2009, 1234/05, *Reklos and Davourlis v. Greece*; ECtHR, 7 February 2012, 40660/08 and 60641/08, von Hannover v. Germany (no. 2).

⁵¹ This distinction should be somewhat qualified since data protection also protects sensitive data.

B. 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.⁵² 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.⁵³ This is one of the reasons we have turned to rights in persona, 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.⁵⁴ 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.

Data protection atomically cuts things up in a technical series of rights and obligations for concrete data processing operations. Rights in persona track the more holistic dimension of the user's digital personae, which arise when different data sources are combined.

Rights in persona also 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).

C. Thirdly and more tentatively, the Databait tools might also provide us with a *technological visualization* 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

⁵² Deliverable 3.11 explores in more detail this mirror side to this investigation: the IP rights of the OSN on the (invisible) parts of the digital persona.

⁵³ There are examples of Facebook denying access request for user data claiming to have 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/>. For a criticism of this position see (Hildebrandt and Van Dijk 2012).

⁵⁴ 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).

mobilize legal qualifications of these datasets as a digital portrait of the user. Here is where the Databait tool might come in handy.

Databait provides an educated guess of the user's digital personae on Online Social Networks.

Through the user interface offered by the web platform (<https://databait.hwcomms.com/welcome>), several 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 some of the user's "incidental data"; and Databait's "user tracker" tool visualizes some of the user's "traffic data" (like cookies and trackers). In this way this tool digitally fleshes out a rough first sketch of the digital portraits that we are speaking about there.⁵⁵ 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.

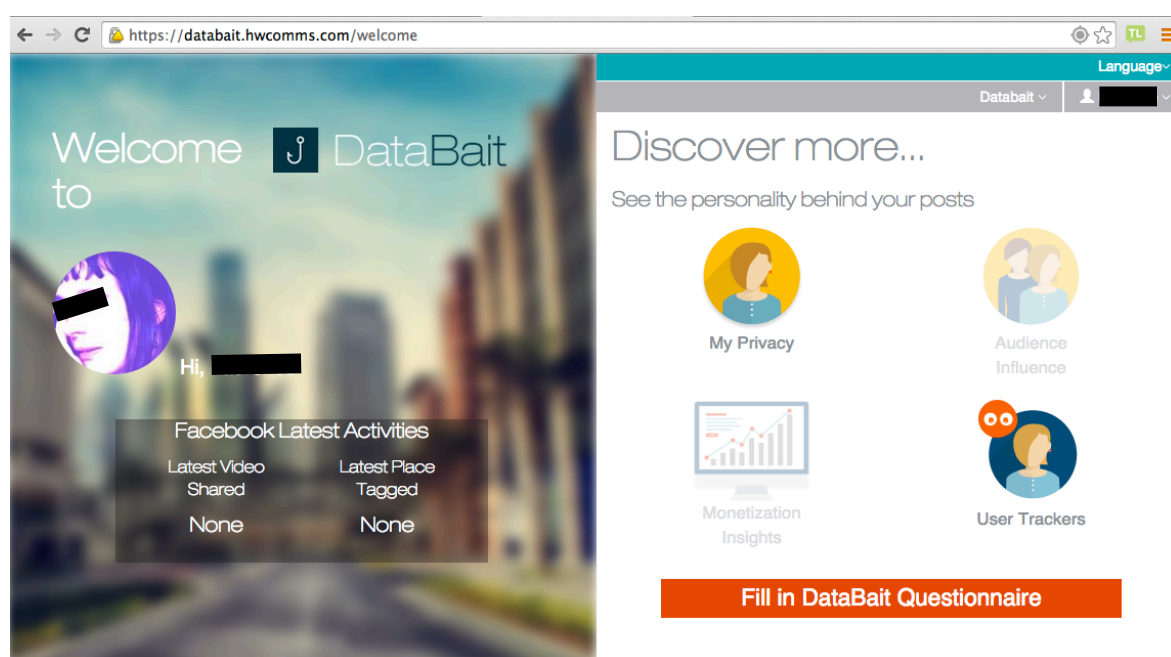


Figure 1. Welcome page of DataBait website (<https://databait.hwcomms.com/>).

⁵⁵ 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.

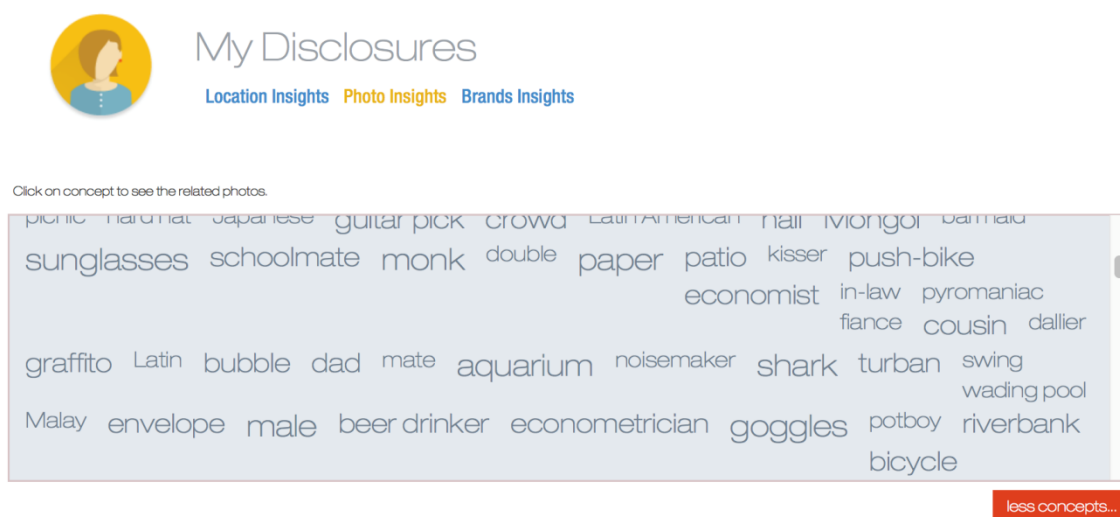


Figure 2. “Photo Insights ” page in the “My Privacy” section on DataBait website.

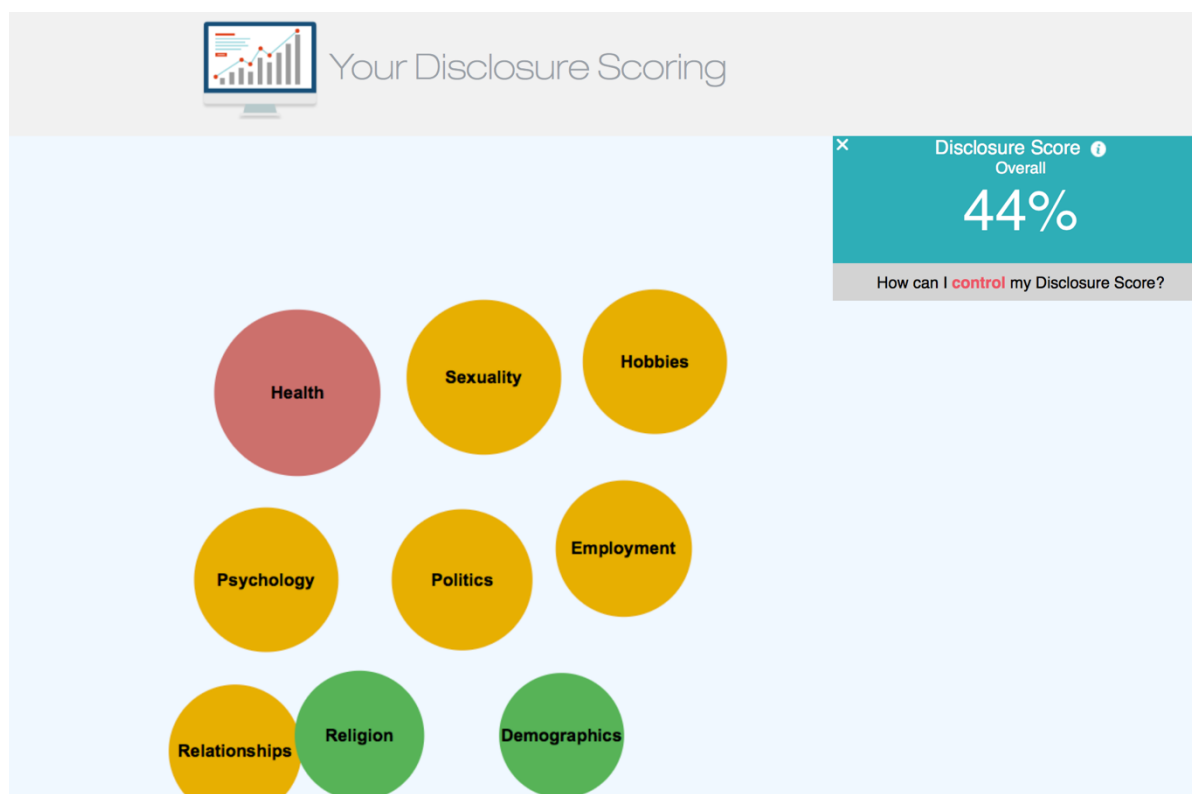


Figure 3 Visualization of the ‘My Privacy score’ (<https://databait.hwcomms.com/>).

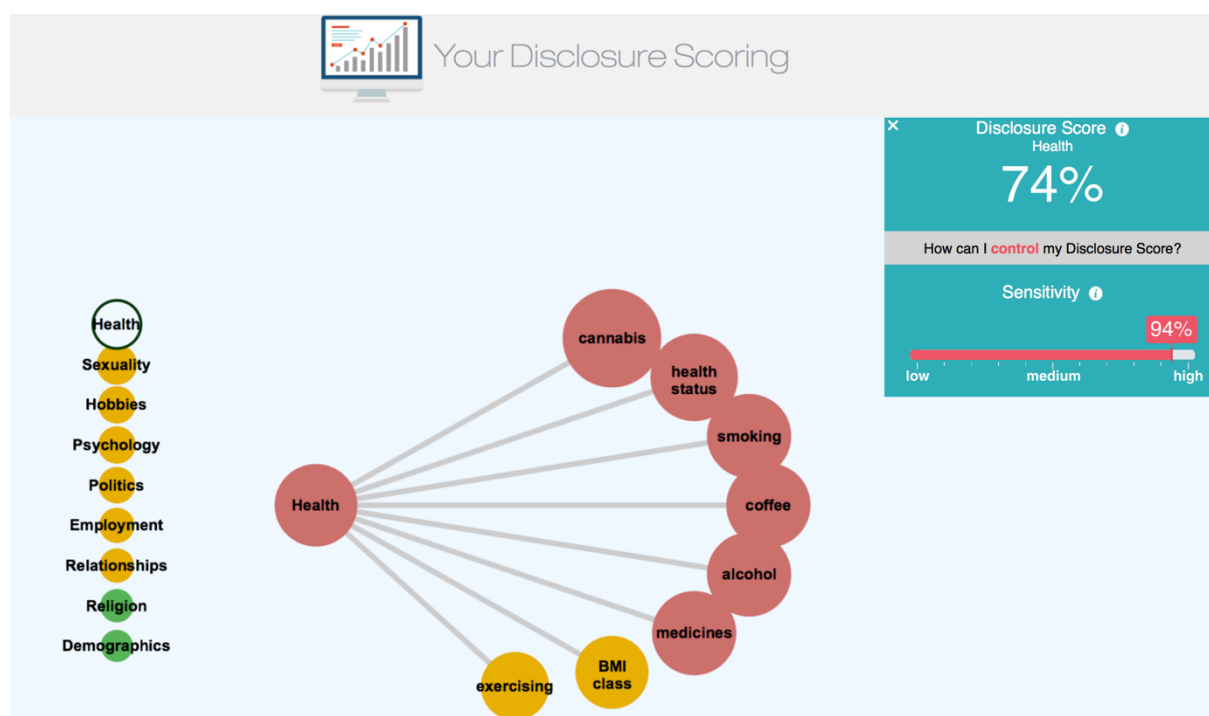


Figure 4 Visualization of the 'My Privacy score' (<https://databait.hwcomms.com/>).

4. Conclusion

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 rights in persona.

With regard to copyright law we distinguish between the potential empowering effects of users copyrights on, firstly, individual pieces of content, secondly, on the visible user profile, and, finally, on the digital persona (consisting of the visible user profile and the “hidden” profile kept by the OSN on a user for, mainly, commercial purposes). It turned out that copyright law is of little avail to users in all of these three regards.

The problem with regard to user empowerment through copyright on individual pieces of content is that users currently often license all their rights away. It should be noted that the broadness and lack of specificity of such IP licenses might potentially render them legally invalid if they would be challenged in court. However, even if OSNs were to adopt licenses with more specific licensing conditions (“the license only allows reproductions for the following purposes :...”), which would be a development we would in itself applaud, they would probably still require the user to license the OSN for profiling purposes (given that advertisement targeting is the core business model of many large OSNs) While adding more specificity to copyright license would resolve the problems that currently surround them from the perspective of copyright law, they would probably still be problematic from the perspective of the new General Data Protection Regulation if using the service provided by an OSN is *conditioned* on consent to such a license. After all, art. 7(4) GDPR, names the conditionality of consent to the processing of personal data that is *not necessary* for the provision of a service as an important factor in assessing whether consent can be considered as freely given. The crucial question would thus be if the reproduction of data for commercial targeting is *necessary* for an OSN service; a question that a Court could very well answer negatively – thereby mandating a paid alternative to the business model that provides an OSN service in exchange for user data. Next to the uncertain status of current copyright licenses, both OSNs as well as researchers (such as the USEMP consortium) who want to use OSN data for profiling purposes have to face the hurdle of third party content (re-posted articles, posts, tweets, photos, music videos, etc.) on an OSN profile. An OSN user cannot license that which is not hers to give. Similarly, the specific copyright clause signed by each DataBait user licensing USEMP to make copies for the purpose of profiling, does not cover third party content. However, infringements on copyrights by USEMP are very unlikely as all our copies are covered by the exception for scientific research, and possibly also by the exception for temporary acts of reproduction. While in the case of DataBait, no copyright issues with regard to copying of individual content for profiling purposes are to be expected, profiling for research purposes within the EU could be simplified in several manners. Firstly, proprietors of copyrights and sui generis database rights could grant liberal licenses to researchers. Secondly, the legislator could create an exception for profiling for research purposes. Finally, the courts and/or the legislator could give a restrictive interpretation to the notion of “reproduction”, so that the copies made for profiling in a non-commercial context fall outside the scope of copyright and database law. Thus, we conclude that while user

empowerment through copyrights on individual pieces of content is made impossible through copyright licenses granted by users to OSNs, copying individual content for profiling purposes by OSNs or independent researchers is no walk in the park either: it is fraught with difficulties because, firstly, the legal validity of current copyright licenses is uncertain and, secondly, because of the presence of third-party content which is not covered by any license.

With regard to the empowering potential of copyright in profiles (both the visible profile and the digital persona) our conclusions are also rather pessimistic. This is 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 have a disempowering effect in these contexts, since such intellectual rights could actually be used against users who want access to their data.

After having concluded that copyrights are of little avail to users who would like to exercise control over the use of their OSN data for commercial profiling, we turn to rights in persona. We explore whether these rights in persona 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 or representations could be argued to work, it is definitively a speculative interpretation. However, 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, rights in persona 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.

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.⁵⁶ 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.⁵⁷ 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**⁵⁸ and their correlated objectification into some of the **basic concepts of the commodity ontology** of online social networks⁵⁹:

- **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.⁶⁰ 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.⁶¹ On Facebook

⁵⁶ 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/>).

⁵⁷ 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.

⁵⁸ 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

⁵⁹ This section is based on research in the EMSOC project (Heyman & van Dijk, 2013).

⁶⁰ This correlate with what Schneier calls service data and disclosed data.

⁶¹ 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 address⁶², 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.⁶³ 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.⁶⁴
- **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."⁶⁵ 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.⁶⁶ 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)

⁶² 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.

⁶³ This correlate with what Schneier calls behavioral data.

⁶⁴ "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.

⁶⁵ <https://www.facebook.com/help/www/453530464730606/>

⁶⁶ <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.⁶⁷ 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.

⁶⁷ 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 Privée 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.
- Brügge-meier, 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., & Schar-tum, 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
- Wauters, E., Lievens, E., & Valcke, P. (2014). Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites. *International Journal of Law and Information Technology*, 22(3), 254-294. doi: 10.1093/ijlit/eau002
- 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