D3.2

Profile transparency, Trade Secrets and Intellectual Property Rights in OSNs – v1

v 1.3 / 2015-03-31

Katja de Vries, Sari Depreeuw, Mireille Hildebrandt (ICIS-RU)

This document relates the analysis of the end users' right to profile transparency (conducted in D3.1) with the database rights and copyright software rights of OSNs and third parties that process user generated data and behavioural data of OSN end users. This report includes some design implications for the DataBait tools, and concludes with a research agenda for the next version of this deliverable (D.3.7) in month 24 of the USEMP Project.

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

Workpackage	WP3
Deliverable lead org.	USEMP
Deliverable type	Report
Authors	Katja de Vries, Sari Depreeuw, Mireille Hildebrandt (iCIS)
Reviewers	Adrian Popescu (CEA), Jo Pierson (iMinds)
Version	1.3
Status	Final
Dissemination level	**PU: Public**
Due date	2014-09-30
Delivery date	2014-10-29
Revision date	2015-03-31

Version	**Changes**
1.0	Initial Release (De Vries)
1.1	Adjustments internal review (Depreeuw, Hildebrandt, De Vries)
1.2	Adjustments after external review by Popescu, Pierson (Depreeuw and Hildebrandt)
1.3	Revised release after EC review

Table of Contents

1.Structure of the legal deliverables in WP3[1]

1.1. Empowerment and compliance

The overall goal of the legal input in Work Package 3 (*Legal Requirements and the Value of Personal Data*) is to elicit/engineer legal requirements that should inform the development of the various USEMP tools. Thus, the legal deliverables in WP3 are not just theoretical legal treatises on data protection, anti-discrimination, and intellectual property rights in relation to the profiles built in and through OSNs, but they aim to provide hands-on input. The first step ("finding the applicable law") in providing legal input is *descriptive*: it is an inventory of the applicable law and how it applies in the case of USEMP. This first step can be further subdivided in three sub-steps:

(i) A concise description of the applicable law;
(ii) An inventory of how the various rights at stake (that is, privacy, data protection, anti-discrimination, copy- and portrait rights of the user and the copy- and database rights of the OSN's and profile building companies) interact with each other;
(iii) An inventory of how the (interactive) functioning of these various rights could affect tools that aim to empower users who are tracked and profiled when browsing the internet and acting in OSNs.

The second step ("putting the law to work to create tools that make the user more empowered while also being compatible with the various rights at stake") of the legal input in WP3 is *constructive*, in that it aims to translate the legal conditions into legal requirements which specify:

(i) how the USEMP tools can contribute best in the effectuation of privacy, data protection, non-discrimination, profile transparency and (possibly) portrait rights. This is about empowerment.

(ii) how to make sure that the USEMP tools are compatible with the legal fields of privacy, data protection, anti-discrimination and intellectual property law. This is about compliance.

The two steps (descriptive and constructive) are not always explicitly distinguished, but they have an implicit structure in writing the legal deliverables of WP3.

1.2. Original legal research and legal coordination support

Despite the fact that all of the legal input in WP3 is quite hands-on, there are some deliverables which provide cutting-edge legal research (D3.1-3.3 and D3.6-3.8; the latter set of deliverables builds on the former) on the operationalization of "legal empowerment" from a multiple rights perspective (see Table 1). The integration of the legal requirements is taken

[1] Because this chapter discusses the overall structure of all the legal deliverables in WP3, it is repeated in the beginning of each of the legal deliverables (currently: D3.1, D3.2 and D3.3).

up in deliverables D3.4 and D3.9 that report on how the legal requirements are interfaced with the tasks at hand in the other WPs (see Figure 1).

	Version 1	Version 2
Fundamental Rights Protection by Design for OSNs	D3.1 (delivery date: M12)	D3.6 (delivery date: M21)
Profile transparency, trade secrets and Intellectual Property rights in OSNs	D3.2 (delivery date: M12)	D3.7 (delivery date: M24)
Copyrights and portrait rights in content posted on OSNs	D3.3 (delivery date: M12)	D3.8 (delivery date: M24)

Table 1: Overview of the deliverables in WP3 containing original legal research

As shown in Figure 1, the legal research (D3.1-3.3 and D.3.6-3.8) and the integration of the legal requirements into the design of the USEMP tools (D3.4 and D.3.9) are intertwined with each other. D3.1-3.3 and D.3.6-3.8 reflect the work done in T3.1-3.5 [M1-M24]. D3.4 and D.3.9 reflect the work done in T3.6, which implements legal coordination.

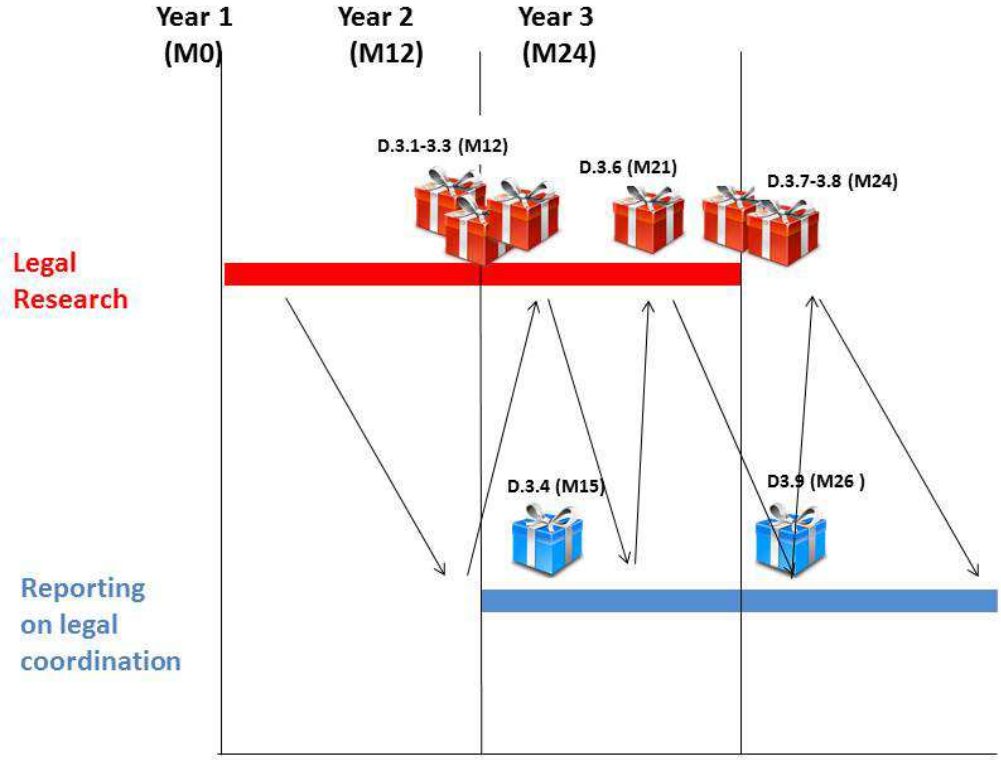

Figure 1. Timeline legal input in USEMP WP3.

1.3. Interaction between the three strands of legal research: the logic of rights trumping each other

With regard to the three strands of legal research ((a) “Fundamental Rights Protection by Design for OSNs”; (b) “Profile transparency, trade secrets and Intellectual Property rights in

OSNs"; and (c) "Copyrights and portrait rights in content posted on OSNs") it is good to mention that these, despite the fact that they are dealt with in separate deliverables, are intertwined as well. They relate to each other as a sequence of cards, where each consecutive card could trump the previous one. Thus, one could say that the *basic* legal compatibility assessment of OSNs is based on a check against data protection, privacy and anti-discriminatory requirements. When creating an application on the internet which tracks and profiles its users, the *first* question to ask is: does it infringe on data protection, privacy and anti-discriminatory requirements by doing so? And if yes: how could one adjust the *design* of the system or practice to prevent this (i.e. fundamental rights protection by design)? These are questions explored in the first step of the legal analysis (D3.1 and D3.6). The *second* question is how the outcome of the first legal step is affected when the rights of others are also taken into account. In the context of USEMP this second step is in particular interesting when profile transparency (a requirement from data protection, i.e. the "first step") is confronted with trade secrets and intellectual property rights (copy- and database rights) of the creators of the system or practice which tracks and profiles its users. With regard to this possible clash of rights, *Data Protection Directive 95/46* states in Recital 41 that:

> Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

And in Recital 51 of the proposed *General Data Protection Regulation* one can find a similar call for a balanced approach:

> Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what estimated period, which recipients receive the data, what is the general logic of the data that are undergoing the processing and what might be the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, such as in relation to the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

Can you have your cake and eat it too? Is it possible for the right to profile transparency to have some bite, if it "should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property"? And what does it mean that the protection of trade secrets or intellectual property rights should not result in the data subject being refused *all* information? Is there indeed a nuanced approach possible where trade secrets or intellectual

property rights only *partly* trump the right to profile transparency? These are questions explored in the second step of a legal compatibility check D3.2 and D3.7). Finally, there is the third step of a legal compatibility check (D3.3 and D3.8), which looks at the copyrights and portrait rights in content of the end-users of OSNs and browsers. In the same way as fundamental rights can be curtailed by trade secrets or intellectual property rights of an OSN, browser or third party tracker-profiler, the protection of the latter could be curtailed ("trumped") by copy-, personality and portrait rights of the end-users of these systems.

The three-fold structure of how the various legal deliverables in WP3 build on each other implies that the *interactive* functioning of the various rights (see above, the first paragraph of this chapter) will *not* be discussed in the first step of the legal analysis (D3.1 and D3.6), but only in the second (D3.2 and D3.7) and third (D3.3 and D3.8).

1.4. A legal compatibility analysis of *what*? The double bind of the USEMP tools as both the subject and the mouthpiece of the law

In constructing the various USEMP tools, end-users are able to gain knowledge about which data are part of their digital trail, what knowledge could be inferred from such data, who is tracking them, to which actors this knowledge could be of interest and what economic value this knowledge could approximately represent. As such the information provided to the end-user of USEMP is one possible example of how legal protection by design could be implemented with regard to systems and practices which track and profile their end-users. The USEMP tools can thus be understood as supportive tools which try to embody *legal protection by design*: not only the requirement of profile transparency as formulated in EU data protection law, but also other legal requirements.

However, the USEMP project and its tools are also a research project which processes many (sensitive) data and which faces the same legal issues as any other data processor. As such, the USEMP consortium is bound by all data protection requirements: it needs to have a proper ground and purpose for the processing of data, process the data in an appropriately secure way, notify the supervisory authority of the processing (at least, if this is required by national data protection law), provide the data subject with all the necessary information about the processing of the data, etc.

Thus, from a legal perspective the USEMP project operates on two levels. On the one hand it tries to embody "legal protection by design" and as such aims to act as the *mouthpiece of the law* (or at least as a technological translation of the law) where OSNs, browsers and third-party profilers are the legal subjects addressed by the law. On the other hand USEMP is also itself a legal subject addressed of the law (at least each and every individual USEMP partner is addressed as such). As a result of this double bind (USEMP is both a translation of and a legal subject addressed by the law), the legal analyses in WP3 operate on two conceptual levels:

(a) the legal compatibility of the tracking and profiling practices performed by OSNs, browsers and third-parties, and the possibility of legal protection by design by tools such as the ones developed by USEMP, and
(b) the legal compatibility of the tracking and profiling practiced by the USEMP tools themselves.

Operating constantly on these two levels of analysis resolves the paradoxical problem that by informing the end-user about the possible “risks” of certain data (showing how sensitive metadata can be inferred: e.g., health or sexual preference from a seemingly “innocent” holiday picture), the USEMP tool itself enters in a field where one has to trod carefully, not to end up infringing fundamental rights while trying to point out (in speculative manner) how such metadata could be extracted by *other* players.

The two levels of the legal analyses in WP3 are nicely exemplified by what was mentioned above (section 1.1) as the two *constructive* forms of legal input, namely that that we need to specify both:

(i) How the USEMP tools can contribute best in the effectuation of privacy, data protection, non-discrimination, profile transparency and (possibly) portrait rights (empowerment).

(ii) How to make sure that the USEMP tools are compatible with the legal fields of privacy, data protection, anti-discrimination and intellectual property law (compliance).

Finally it should be noted that when looking at the legal compatibility between (a) the tracking and profiling practices the USEMP tool and (b) the requirements following from privacy, data protection, anti-discrimination and intellectual property law, the legal analyses also give insight about how legal compatibility would be affected if tools similar to those created by the USEMP project would be commercialized. Within the USEMP project much of data processing and profiling is allowed precisely because the purpose of the processing is purely scientific – but what would happen if (after the end of the project) these tools would still be used and they would be no longer fall under exemptions of scientific research? On top of distinguishing the two aforementioned conceptual levels of legal analysis, we should add that there are two sub-levels which can be distinguished within the second level:

(a) the legal compatibility of the tracking and profiling practices performed by OSNs, browsers and third-parties, and the possibility of legal protection by design by tools such as the ones developed by USEMP, and
(b) the legal compatibility of the tracking and profiling practices of the USEMP tools themselves.
    (i) the legal compatibility of the tracking and profiling practices of the USEMP tools as they are now, that is: processing data with the sole purpose of scientific research;
    (ii) the legal compatibility of the tracking and profiling practices of the USEMP tools as they could hypothetically be in the future, that is: commercialized and no longer part of a research project.

1.5. First and second versions of the legal research deliverables

As shown in table 1 the three strands of legal research result in six deliverables. After the first year each strand of legal research results in intermediate reports (D3.1-3.3), that will be further developed into three final reports in the second version at the end of the second year, taking into account the progression on the technical side (D3.6-3.9). D3.4 and 3.9 form the interface between the legal requirements and the technical specifications of the DataBait

tools. In the current deliverable 3.1 we have added an annex with a first version of the integration tables[2] that will be presented in 3.4.

[2] The integration tables in D3.4 contain legal qualifications of the data/content processed within the USEMP project, the requirements which are derived from these qualifications and their embodiment in the technical specifications of the DataBait tools. The qualifications and requirements follow from the various legal fields studied with regard to the USEMP project (notably data protection, antidiscrimination, copyright, sui generis database right and portrait rights derived from Art. 8 ECHR). The preliminary integration tables in annex B of this deliverable only regard requirements following EU data protection requirements and a little bit of EU antidiscrimination law.

2. Tensions between profile transparency and the rights of the profilers

2.1. The profile as subject matter protected under IP rights

In D.3.1 we explored several ways in which user empowerment towards the commercial profiling of one's digital trail when using social networks or a browser can be translated into the protection granted by European fundamental rights. Thus, the spotlight was on the legal relationship between an individual end-user of a social network or a browser and (part of) the profiling operations to which this end-user is subjected.

Depending on the legal regime invoked, the legal qualification of the end-user and the relevant part of the profiling operations will differ. For example, when the EU data protection regime is invoked the end-user will be qualified as a *data subject* ("an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", Art. 2(1) DPD 95/46[3]) with a claim of transparency with regard to the *profiling based on his or her personal data* (Art.15(1) in conjunction with Art. 12(a) DPD 95/46). In contrast, when the EU anti-discrimination regime is invoked the same individual will legally be qualified as a potential *victim of discriminatory measures* and the discriminatory part of the profile may be qualified as a *prohibited ground for discrimination*. Therefore, one user can have several legal relations to what appears in day-to-day life as the same object (the profile).

In D3.1 the commercial (the social network, the browser, and third parties) and scientific (USEMP consortium) actors that are engaged in profiling were only presented as ancillary actors in shaping the legal relation between end-user and the profile: either helping or inhibiting profile transparency; either contributing to discrimination or combatting it through information; etc. However, when the field of intellectual property (IP) rights is taken into account, each of these profilers may also have one or more autonomous legal relations towards a "profile": for example, a copyright towards the profile, or a trade secret or database right towards the way in which a profile is organised. Legally speaking one profile could thus exist simultaneously in multiple ways: it can be a profile (as defined by data protection law), a ground for prohibited discrimination, a trade secret, a database, a copyrighted work, the object of a contract, etc. (see figure 1).

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23/11/1995, p. 31-50. The DPD 95/46/EC is currently the main legal instrument regarding general data protection, but is in the process of being replaced by the proposed General Data Protection Regulation, which will probably enter into force in 2016.

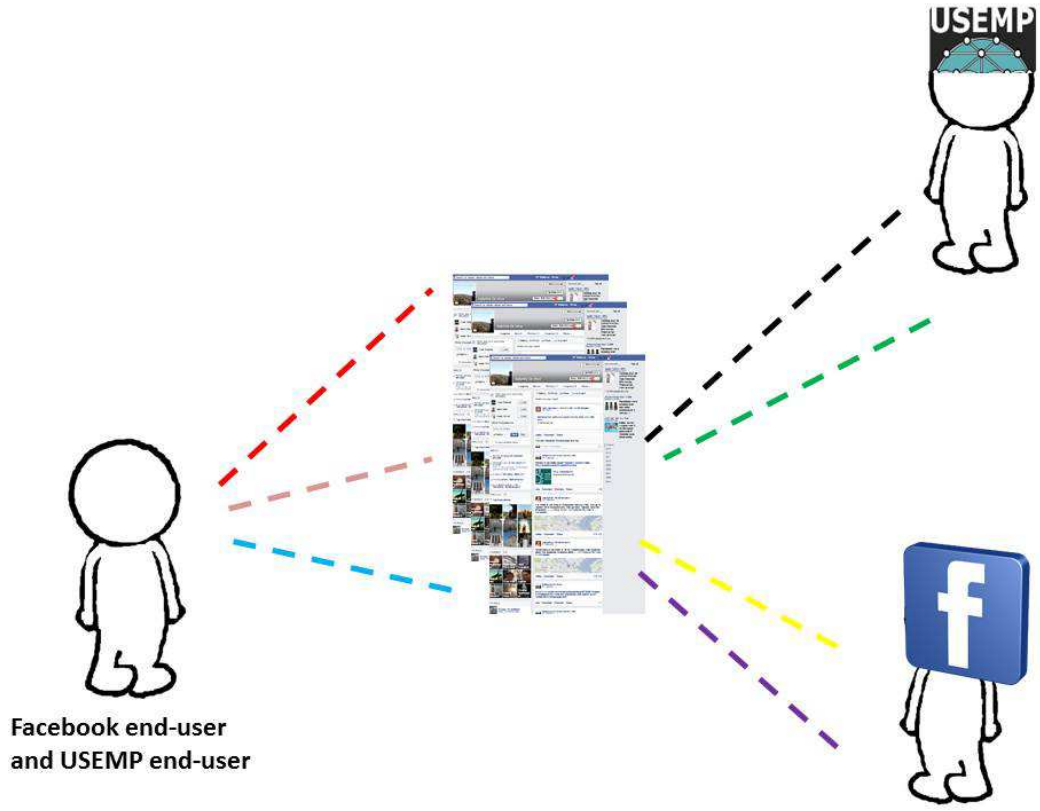

Figure 2: The "same" profile can be the object of various legal relations with multiple actors.

Often several legal relations can co-exist but sometimes they will clash: for example, the intellectual property rights of a commercial profiler who wants to protect the algorithm used to offer targeted ads might seem incompatible with the rights of the data subject to have access to the logic of the profiling. Anticipating these kinds of conflicts of interest, Recital 41 of the DPD 95/46 states that although the right of access "must not adversely affect trade secrets or intellectual property rights in particular the copyright protecting the software [..] these considerations must not, however, result in the data subject being refused all information." Even though there is quite an abundance of case law in which a balance had to be struck between an IP right and a fundamental right (for example cases involving parodies of copyrighted works, where a balance had to be struck between copyright protection and freedom of expression[4]), up until now there is no case law where IP rights in profiling and data protection law are confronted with each other[5]. This is not surprising, given the highly unclear IP status of profiles: whether a "profile" can be legally qualified as a copyrighted

[4] *Ashby Donald and others v. France*, Appl. nr. 36769/08, ECtHR (5th section), Strasbourg 10 January 2013 ; *Deckmyn v. Vandersteen*, C-201/13, EU:C:2014:2132.

[5] Van Dijk names three cases of which the subject matter might be extended in an analogical manner to a potential clash between IP-rights on a profile and profile transparency rights : ECHR, *Gaskin v. UK*, Application no. 10454/83, 7 July 1989 [scope of the right of access to care records kept by the public authorities with regard to the time Gaskin spend in public care during his childhood]; *Dexia*, The High Court of the Netherlands (Hoge Raad) [scope of the right of access to one's financial file at *Dexia* bank] , 29 June 2007, LJN: AZ4664, R06/046HR; and *Opinion of the Dutch Data protection Authority (CBP) regarding the right of access to the raw data of a psychological test and the IP rights protecting such a test*, 15 July 2008, online available at http://www.cbpweb.nl/downloads_overig/NIP.pdf.

work, as a database protected by either copyright or the *sui generis* database right, or as the object of trade secrets is far from undisputed (Custers, 2009, section 5.3; Van Dijk, 2009 2010a, 2010b).

A first problem to be solved when asking if "a profile" can be qualified as the object of a trade secret or the aforementioned IP rights, is that the noun "profile" is even more equivocal than the verb "to profile". "Profiling", as explained in D3.1, is defined in the proposed GDPR as:

> … any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. (Art. 4-3a of the proposed *General Data Protection Regulation*[6] [pGDPR], the successor to DPD 95/46)

Contrary to the verb "profiling" (which is already hard to define`, see e.g.: Hildebrandt, 2008; Ferraris, 2013), there is no legal definition of what "a profile" is. However, there are two meanings which stand out: in the first place it can refer to **an individual set of characteristics** (e.g., a Facebook profile consisting of volunteered data on the fronted, but including observed data at the backend), and secondly it can refer to what could be termed a **data model** (usually referred to as an "algorithm" which classifies individuals according to certain traits or preferences (e.g., a data model which predicts a user's political preferences based on Facebook posts). The profile of an individual on an SNS can be protected under intellectual property rights (IPRs) such as copyright or database rights[7] which implies that the holder of the IPR can exercise exclusive rights on certain uses of the profile. The act of

[6] The proposed *General Data Protection Regulation* (pGDPR) is currently being created in the so-called *ordinary legislative procedure* (formally known as the *codecision procedure*) of the EU, which is basically a bicameral legislative procedure : it gives the same weight to the European Parliament and the Council of the European Union (consisting of ministers from the 28 EU Member State governments). The GPDR was first proposed on 25 January 2012 by the European Commission (that is, the executive branch of the EU and the only EU institution empowered to initiate legislation) and now has to be jointly adopted by the European Parliament and the Council. The text proposed by the Commission [*Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25 January 2012, COM(2012) 11 final] has been subjected to a first reading by the European Parliament and has been amended the on 12 March 2014 [*European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Strasbourg, 12 March 2014, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), online available at : <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>]. Currently, the amended text is examined by the Council of the European Union. If Parliament and Council disagree on a proposed legislative text, it can go back and forth between Parliament and Council up to three times. A clear infographic clarifying the ordinary legislative procedure can be found here : <http://www.europarl.europa.eu/aboutparliament/en/0081f4b3c7/Law-making-procedures-in-detail.html> [last accessed 29 September 2014]. Looking at the current status of the proposed General Data Protection Regulation and the steps in the legislative procedure which are still ahead of it, the GPDR will most likely enter into force by 2016.

[7] It is not very likely that a user profile be protected as a trade secret, since all information from the user is actually visible to others and thus not very 'secretive' (see below section 2.2). If, however, an OSN develops user profiles that contain behavioural data to which users have no access, such profiles will probably be kept a secret.

gathering data from individual profiles may also result in databases, which may themselves (as a structured unity of data) be subject to intellectual rights. Moreover, as training sets, these databases can contribute to the creation of machine learning algorithms (which may then be embedded in computer programs which have the ability to profile), or to the resulting data models (in the sense of "profiles") which computer programs and profiles in turn can both be subject to IPR protection.

Thus, exploring whether *profiling* amounts to an infringement on trade secrets or certain IP rights in fact entails three questions:

(1) does the **profiling process** involve infringements on intangibles that are traditionally qualified as trade secrets or the objects of certain IP rights (e.g. a set of pictures from a Facebook profile which is copied in order to make profiling possible)?,
(2) can an **individual profile** (e.g. the complete Facebook profile of a user, potentially including both user generated content and behavioural data) be qualified as a trade secret or the object of certain IP rights?,[8]
(3) can **data models** (e.g. image classifiers) be qualified as trade secrets or the objects of certain IP rights?

In order to answer these questions we will have to take a closer look at the notions "trade secret", "patent", "copyright", and "*sui generis* database right". The answers to these questions have large implications for the USEMP project, because they might either support or interfere with the goal of the DataBait tools to provide profile transparency and give insight into possible discriminatory differentiations and illegitimate negative stereotyping. For USEMP it is pivotal to know if the user rights it aims to support are "trumped" by IPR rights.

The analysis of IPR rights commonly takes the following issues into consideration (i) the protected subject matter, (ii) ownership issues (first owner, transfer of rights), (iii) scope of protection: protected acts and exceptions, term of protection; (iv) enforcement. While in D3.2 the issues are rather the protected subject matter (e.g. are there protected databases or other works?) and the scope of protection (e.g. is there a reproduction of a protected element? is there an extraction of a protected section ? do exceptions cover these protected acts?), the issues in D3.3 are more related to ownership and the valid transfer/licensing of rights by users/authors. When signing up for Facebook you sign the terms and conditions in which you agree to a number of IP issues (including the non-exclusive license to Facebook for all your IP-matter). Thus, when studying the issues related to copyrights/database rights of the users it is important to look at the terms and conditions of the agreement between the OSN and the users (Wauters e.a., 2014).

Thus, this deliverable D3.2 will explore the different types of rights that OSNs, browsers and third-party profilers might have in profiles. We discuss four possible legal qualifications with which these actors might protect the economic, intellectual and creative efforts which they have invested in 'profiles' of OSN and browser users: trade secrets, patentable inventions, copyrights and the IP protection of databases. It should be born in mind that this analysis does not only analyze how these legal means allow OSN providers and other profilers to act

[8] Note that on the foreground a user profile consists of volunteered data (user generated content), whereas the profile at the backend of the system will probably also consist of observed data (machine readable behavioural data).

towards the users of their tools and services, but also which legal limits these means impose on makers of empowering transparency tools such as the Databait tools.

2.2. Profiles as trade secrets?

Let us begin by explaining what is (seemingly) the most straightforward term: a trade secret. A trade secret is originally not a legal term but the result of a factual action: it is a secret which is kept by a company in order to keep an economic advantage over competitors.

> 'Trade secret' means information which meets all of the following requirements:
>
> (a) is **secret** in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) has **commercial value** because it is secret;
>
> (c) has been subject to **reasonable steps** under the circumstances, by the person lawfully in control of the information, to **keep it secret**. (Art. 39(2) TRIPS[9]; Art. 2(1) of the proposed *Trade Secret Directive*[10] - our emphasis)

The exact recipe of *Coca Cola* is an example of a trade secret. Keeping a trade secret is a practical solution which avoids the legal complexities and the high costs and publicity of a patent.

However, if a trade secret is stolen the law might get involved after all, when a remedy is needed to compensate for the financial losses incurred. It is in this stage that a judge might be called upon to decide whether something was a true trade secret or not. Although the TRIPS Agreement obliges Member States to provide a minimum protection for undisclosed information, including trade secrets, there is currently no unified EU legislation with regard to trade secrets and national laws differ very much in their definitions, in the type of legislation that affords protection and the scope of protection granted[11]. Member States provide protection under specific laws on trade secrets, unfair competition, intellectual property, civil code/tort law, labour law, contract law, criminal law or common law provisions.

---

[9] World Trade Organisation's 1994 Marrakesh Declaration, Annex 1C *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS). The TRIPS Agreement is a multilateral agreement on intellectual property which was drafted by the World Trade Organisation and came into effect on 1 January 1995. It is defines a set of minimum standards for many forms of intellectual property rights (e.g. copyrights, trademarks, and trade secrets) which binds all 158 WTO members. As such it is a very important and comprehensive instrument with regard to all kinds of IPRs. When comparing the TRIPS agreement with other important international IPR agreements, such as the *Berne Convention for the Protection of Literary and Artistic Works* ("the Berne Convention") from 1886, it is not only its extremely broad geographical reach but especially the fact that (a) it covers almost all forms of IPRs (for example, the aforementioned Berne Convention only covers copyright), and (b) that it incorporates most substantial provisions from several other important IPR agreements (such as the aforementioned Berne Convention), which makes it stand out. As such the TRIPS agreement is an extremely *comprehensive* legal IPR instrument.

[10] Proposal for a Directive of the European parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure ("Proposed Trade Secret Directive"). COM/2013/0813 final - 2013/0402 (COD). Brussels, 28 November 2013.

[11] See Baker & McKenzie 2013.

The proposed EU Directive on Trade Secrets tries to bring more unity. The legal definition of a trade secret in the proposed EU Directive is very broad: a trade secret can be basically any know-how in any field (commercial or technical information) which has commercial value as long as it can be shown that the keeper of the secret has made appropriate efforts to keep the secret a secret. One cannot claim protection for something that one has not tried to keep secret by taking "reasonable steps". Futile steps or mere *pro forma* measures are not sufficient. The broadness of the definition of a trade secret means that, for example, a data "model" (which can refer to one type of "profile"), but also the "training set" as structured in a relational database ("the ingredients" in their respective "containers") on which a model is built (Ateniese, 2013) and the machine learning algorithm (the "recipe" which is used to construct the model), could very well be trade secrets. As exemplified by figure 2, a data "model" or an "algorithm" bear a likeness to a recipe such as the one for Coca Cola: while everybody knows what the approximate ingredients are, the competitive advantage is exactly in the details ("the secret ingredients", their measurement and how they interact). Thus, while the main ingredients of the Facebook news feed algorithm are well known, it's the details which are protected as a trade secret.

Under the national laws, the **scope of trade secrets protection** and the available remedies are quite divergent. Generally, the owner of the trade secret must establish that the trade secret has been infringed and that the information was used or misappropriated in an unlawful way. The specific conditions depend however on the legal instrument that the trade secret owner relies on, e.g. labour law or tort law against a (former) employee or unfair competition law against a competitor.

The proposed Trade Secrets Directive intends to harmonise the protection against the "unlawful acquisition, use or disclosure of a trade secret" (art. 3 proposed Directive)[12]. The **acquisition** of trade secrets is considered unlawful if it is carried out, without the consent of the trade secret holder, intentionally or with gross negligence by (a) unauthorised access to files under control of the trade secret holder that contain the trade secret, (b) theft, (c) bribery, (d) deception, (e) breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy, or (f) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

Furthermore, the **use** or **disclosure** of such acquired information is unlawful if it is carried out, without the consent of the trade secret holder, intentionally or with gross negligence, by a person who (a) has acquired the trade secret unlawfully; (b) is in breach of a confidentiality agreement or any other duty to maintain secrecy of the trade secret; or (c) is in breach of a contractual or any other duty to limit the use of the trade secret. More generally, the use or disclosure of a trade secret is considered unlawful "in the second degree", when the user of the secret information, at the time of use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully. Further down the line, it is considered unlawful to proceed to the conscious and deliberate production, offering or placing on the market of infringing goods, import, export or storage of infringing goods for those purposes.

[12] The Directive has not been adopted yet – let alone transposed in the internal legal order of the Member States. Considering the divergence among the national regimes on this point, we will restrict the analysis for now to the provisions of the proposed Directive. Should more specific questions arise, we can analyse these according to the applicable law.

In contrast, under the proposed Directive, the holder of the trade secret has no legal basis if the information is acquired in a lawful way, i.e. by independent discovery or creation, by observation, study, disassembly or test of a product or object that has been made available to the public or that it is lawfully in the possession of the acquirer of the information, by exercise of the right of workers representatives to information and consultation in accordance with European Union and national law and/or practices or by any other practice which, under the circumstances, is in conformity with honest commercial practices (art. 4 proposed Directive). Finally, the proposed Directive contains provisions that limit the rights of trade secret holders, in favour of *inter alia* the legitimate exercise of the right of freedom of expression and information or in order to address the misconduct, wrongdoing or illegal activity of the trade secret holder (art. 5 proposed Directive).

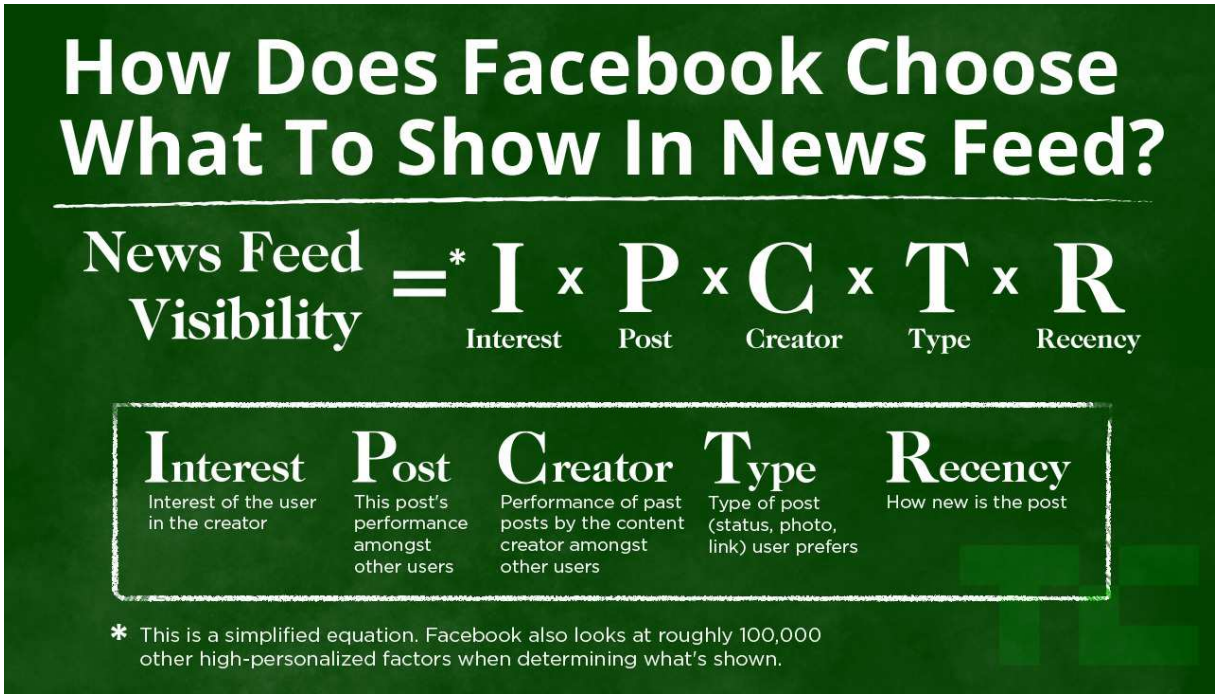

Figure 3: A simplified depiction of the algorithm which is used by Facebook to decide what is shown in the News Feed of a user. Image source: <http://techcrunch.com/2014/04/03/the-filtered-feed-problem/>

If we apply these rules to (i) the profiles and (ii) the act of profiling, we come to the following provisional conclusions.

Regarding the data derived from an individual Facebook profile: as long as this profile is just a small amount of (relatively) publicly accessible "raw data" (volunteered data) it is not very likely that it would qualify as a trade secret. Firstly, this is the Facebook profile that is published by its owner hence it is not secret. Secondly, taken on their own these profiles are not likely to represent a commercial advantage. The Facebook user cannot claim protection for her profile as a tradesecret. However, to the extent that Facebook adds machine-readable behavioural data to their individual user profiles - to which users have no access - the OSN might claim indeed a trade secret. The combination of volunteered, behavioural and inferred data contained in the individual profile that is only accessible to the OSN thus results in valuable knowhow that could qualify for protection as a tradesecret. Notably when an individual Facebook profile contains historical data which neither the Facebook account

holder nor others can see. Such information could have commercial and technical value and if Facebook takes reasonable steps to keep these data secret, then Facebook could indeed claim protection of this information, as a trade secret.

So what about extracting large amounts of data from a browser or a social network site? If these data can be used to train a competitive algorithm, this collection of data probably could be qualified as a trade secret, along with the precise training method and the analysis of the results – however, the crucial question will be how secretively these data have kept.

When creating profile transparency tools like those developed in USEMP it is important not to infringe on trade secrets. Because the inferred knowledge presented in the USEMP tools is based on machine learning algorithms and data models developed within the USEMP consortium, it seems highly unlikely that this could be qualified as an infringement on a trade secret. An actual risk of infringing trade secrets (depending on the applicable law) is present, rather when one would try to hack into protected information, to obtain secret information by illegally accessing secured systems or by manipulating employees or service providers to provide such information .

It is unlikely that the intended research of the USEMP consortium amounts to an infringement of Facebook's trade secrets. The USEMP research will not be based on unlawful access to Facebook's files, it will not approach Facebook intimi to share secret information in breach of their confidentiality agreements. Instead, the inferences made in USEMP are hypothetical ("this is the kind of information which *could* be extracted from your data trail and this is what it *could* be used for"). After all, these inferences are based on independent discovery, observation and study (see art. 4(1) proposed Directive). Moreover, the legitimate exercise of the right to freedom of information and expression could be invoked in defence (art 4(2) proposed Directive).

2.3. Profiles as patentable inventions?

As an alternative to keeping a data model as a trade secret, one could also try to patent it as a patentable invention[13], that is as a novel and inventive (i.e., non-obvious for somebody acquainted with the state of the art) product, apparatus or a process that has industrial applicability. The way to patent an algorithm would be to frame it as more than "just" an algorithm, but to patent the product, apparatus or process to which it belongs. For example, the famous Google *PageRank* algorithm is a patented invention within the US.[14] Whether algorithms can be patented is a highly contentious legal topic, which is further complicated by differences between patent law in, for example, the US and the EU. Within the EU, computer programs and mathematical methods are explicitly named as being *outside* the scope of what can be qualified as a patentable invention (Art. 52(2a) and(2b) European Patent Convention, EPC).

[13] European Patent Convention, 5 October 1973.

[14] *U.S. Patent No. 6,285,999 on a method for node ranking in a linked database*, invented by Lawrence Page, assigned to Stanford University, filed for on January 9, 1998. See : http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6,285,999.PN.&OS=PN/6,285,999&RS=PN/6,285,999.

Art. 52. Patentable inventions .

(1) European patents shall be granted for any inventions which are susceptible of industrial application, which are new and which involve an inventive step.

(2) The following in particular shall not be regarded as inventions within the meaning of paragraph 1:

a. discoveries, scientific theories and mathematical methods;
b. aesthetic creations;
c. schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;
d. presentations of information.

(3) The provisions of paragraph 2 shall exclude patentability of the subject-matter or activities referred to in that provision only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such.

On the basis of Art. 53(3) EPC patents are restricted to technical solutions.

> "computer languages or codes are considered computer programs as such and receive copyright protection. The technical solution to a technical problem that a computer program may provide is not considered to be the computer program as such, but refers to its function. If it has a technical function or "character" it is patentable as an invention." (Custers, 2009, p. 48)

Apart from the fact that within the context of the EU data models or algorithms are probably not patentable, patenting also brings along two characteristics which may render it an unattractive option for the "inventor" of a data model. Firstly it requires a considerable investment of time, money and work to file a patent (contrary to copyright, which comes into existence automatically whenever a copyrightable work is created). Secondly a successful patent application requires that the invention is disclosed to the public. It is precisely this publicity of the invention which gives the inventor the exclusive right to exclude others from the use of the invention.

The publicity of patents could also mean that the rights on a patented data model are unlikely to interfere with the right to profile transparency: a data subject who is subjected to such patented profiling could simply access the patent and read about the logic underlying the profiling. While the technical language used in a patent description will not be easy to grasp for every user, it can be used by technically skilled providers of transparency tools as a basis for a more comprehensible and easy description of the logic underlying the profiling. Clearly, one could question if such a general description suffices to provide the necessary profile transparency. In fact it might be more interesting to know which specific data of the data subject have been used: the usefulness of a general description of the logic underlying the profiling will largely depend on whether the data subject has access to such additional information.

For an OSN provider, disclosing the algorithms behind their advertising strategies could weaken their market position, even if reverse engineering would constitute a violation of the patent. Facebook has several patents and patent applications in Europe (as well as in the US).

For our research it is interesting to note that insofar as, for instance, artificial neural networks, are a hybrid of hardware and software, they may indeed be patentable elements under the EPC, since they may provide technical solutions. It is also interesting to note that the distinction between computer science and electrical engineering that seems to underlie the restrictions of the EPC, is crumbling as wearables, sensor-technologies, and the Internet of Things integrate with back-end systems that include neural nets, thus further hybridizing software and hardware. In the context of USEMP this would, however, only be relevant insofar as either Facebook or USEMP partners employ hybrid systems to develop profiles.

Considering that OSN providers, such as Facebook, use a combination of copyright, patent and trade secret protection to maximise protection of its services, the next version of this deliverable will examine to which extent OSN providers could rely on these protective rights to oppose the development, offer and use of transparency tools (such as DataBait). It is not our purpose to examine in detail whether the DataBait tools or the activities of the USEMP partners infringe any of the actual patents owned by Facebook or other parties. Instead, it will be briefly verified whether these tools could exempted under any of the applicable exceptions, such as the research exception.

2.4. Profiling and copyright?

Intellectual property rights (such as patents, copyrights and *sui generis* data base rights) are, contrary to “ordinary” property rights, not based on something “material” but on an “intangible” product of the mind like a particular expression (copyright) or invention (patent). Being the *owner* of a book only means that one owns the book as a “material object” and does not imply that one also has the intellectual property rights on the novel contained by the book, or that one is entitled to copying the book, to sharing it with one’s friends or adapting it into a play or a film (though exceptions are often made for sharing within a small set of people).

In this deliverable, we will examine whether an OSN operator holds any copyrights on its system and whether it could rely on any exclusive rights under copyright to prohibit transparency efforts. In the next deliverable (D3.3) we will research whether the user of a social networking service can invoke her copyrights to strengthen her legal position.

The **subject matter** protected under copyright is not uniformly defined[15] but indications can be found in various legal instruments, such as the Berne Convention, the 1996 WIPO Copyright Treaty and, at EU level, the Directives in the field of copyright. Copyright can offer protection for divers types of creations in the literary, scientific and artistic domain: books, theatre plays, operas, music and lyrics, dance choreographies, press articles or scientific publications (art. 2 BC). Moreover, computer programs are considered literary works and

[15] Copyright is granted at the national level and is regulated in national laws but many harmonisation efforts have been made at the international and European levels.

therefore protected under copyright (art. 4 WCT; art. 1 CPD[16]) and certain aspects of a database may also be protected under copyright[17].

A copyright cannot be based on a mere idea (e.g., a guy and a girl fall in love with each other but their respective families have a feud), but only on a particular expression of an idea (Shakespeare's *Romeo and Julia* is very unique *expression* of the aforementioned idea).

> Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.[18]

Some differences may subsist in the definition of the "work", i.e. the protected subject matter of copyright, but one can broadly say that in order to be a copyrightable, the subject matter should be "**original**" or the author's own "intellectual creation"[19] and reflect the author's personality[20]. More specifically, this is the case if the author was able to express his or her creative abilities in the production of the work by making free and creative choices[21].

Any OSN will present several elements that qualify for copyright protection. Firstly, the presentation of the OSN may be protected under copyright, in particular the graphic user interfaces. In addition, its computer programs (i.e. source code, object code, and interfaces) are likely to be original and therefore protected under copyright. Its databases may enjoy some degree of protection under copyright as well. In short, any OSN deals with copyrights on various types of creations and from various sources (its own creations, user contributions, third party content shared by users). Furthermore, protected subject matter from other sources than the OSN may be used during the development of the DataBait tools, e.g. images that are part of "training sets". It will be verified in D3.4 (and its final version, D3.9) whether such third sources are used and on which legal basis (exception, consent).

Secondly, users post elements that are "original" ("user generated content", such as status updates, pictures – even "selfies" – or music). In its general terms and conditions Facebook requires the user to grant a broad licence, which could mean that Facebook is entitled to exercise copyright rights on content submitted by its users (this aspect is discussed in D3.3 and will be further explored in the next version of this deliverable, D3.8).

The **scope of protection** of copyright is determined by the exclusive rights granted and the exceptions. Holding the copyright over a work means, according to the *EU Copyright* or *"Infosoc" Directive*[22], to hold the right over its reproduction[23], publication[24] and distribution.[25]

---

[16] **Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version),** *OJ* L 111, 5.5.2009, p. 16–22 (hereafter CPD).

[17] **Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases,** *O.J. L 077 , 27/03/1996 P. 0020 – 0028 (hereafter DBD);*

[18] Art. 2, *WIPO Copyright Treaty*, adopted 20 December 1996, Geneva.

[19] Judgment in *Infopaq International A/S v Danske Dagblades Forening*, C-5/08, ECLI:EU:C:2009:465, para. 37.

[20] Recital 17 in the preamble to **Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights ,** *O.J. L 290 , 24/11/1993 P. 0009 – 0013 ;*

[21] Judgment in *Eva-Maria Painer v Standard VerlagsGmbH and Others*, C-145/10, ECLI:EU:C:2011:798, para. 89.

[22] 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, O.J. L 167, 22/06/2001 P. 0010 – 0019.

Based on the technical description of the DataBait tools, it will be verified in D3.4 (and D3.9) to which extent any acts of reproduction, distribution or communication to the public are performed during the development and operation of the DataBait tools.. Should it be found that no exception applies, a licence from the rightholder should cover the USEMP activities.

The exceptions to the exclusive rights are listed in art. 5 InfoSoc Directive. During the phase of development of the transparency tool, the exceptions for scientific research may be interesting for the USEMP consortium (art. 5(3)(a) InfoSoc Directive[26,27]. It should however be verified in the applicable national law which exceptions have been transposed and under which conditions. Considering the condition that the exception only covers the use of works "to the extent justified by the non-commercial purpose to be achieved", it is unlikely that the exception provides a legal basis for commercial usage of the DataBait tools.

In the next version of this deliverable (D3.7), we will analyse whether any exception applies to the DataBait tools, considering the circumstances in which they are developed and will be used.

---

[23] Article 2. Reproduction right.
Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:
(a) for authors, of their works;
(b) for performers, of fixations of their performances;
(c) for phonogram producers, of their phonograms;
(d) for the producers of the first fixations of films, in respect of the original and copies of their films;
(e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

[24] Article 3. Right of communication to the public of works and right of making available to the public other subject-matter.
1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.
2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
(a) for performers, of fixations of their performances;
(b) for phonogram producers, of their phonograms;
(c) for the producers of the first fixations of films, of the original and copies of their films;
(d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.
3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

[25] Article 4. Distribution right
1. Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.
2. The distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.

[26] Article 5 Exceptions and Limitations (…)
3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:
(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;

[27] The InfoSoc Directive does not provide an equivalent exception to the exception for decompilation (in view of developing an interoperable software) in the Computer Programs Directive (art. 6 CPD).

The Computer Programs Directive harmonises the protection of computer programs under copyright[28] and grants rights of reproduction, adaptation and distribution (art. 4 CPD). Exceptions are provided for "normal use", back-up copies, observation and testing (art. 5 CPD) and decompilation (art. 6 CPD).

As far as the computer programs of the OSN are concerned, we will verify in D3.4 (andD3.9)), based on the technical description of the development and use of the DataBait tools, whether any protected part of the computer programs running the OSN will be used and, if so, an exception can be relied on.

Generally, the author – the person who has created the work – is the first **owner** of the copyrights[29]. The author will often rely on a professional – commercial – partner for the exploitation of the work and thus grant rights to the publisher, the record label or film producer. In our present media environment, authors can also share their works with their interested public via social platforms, which often provide a copyright clause in the terms and conditions of their services. The main focus of this deliverable (D3.2) are those IP rights of which the OSN is the first owner – in contrast to D3.3 where the IP rights are discussed of which the OSN user is the first owner. However, because we want the to list *all* the IP-rights of the OSN in this deliverable a slight conflation between the thematic of D3.2 and D3.3 is unavoidable : after all, an important part of the IP rights of the OSN is derived through a license from the OSN-user.Thus we need to dedicate some attention here to the ownership of the content submitted by users to Facebook – this is relevant for both this deliverable (D3.2) and D3.3. In the hypothesis that the development and operation of DataBait entails restricted acts (reproduction) relating to protected content and no exception applies to such activities, then USEMP should seek the consent of the right holder of the used content. If the users have validly transferred their copyrights in the posted content to Facebook, then Facebook can grant or refuse such licence. If the copyrights cannot be validly transferred by the Facebook general terms and conditions, then the consent of the individual right holders (not necessarily the user) should be acquired. This would entail many practical complications.

Thus it is crucial to establish whether the transfer of the copyright by the OSN users is valid or not. In Article 2 of the *Facebook Statement of Rights and Responsibilities*[30] (version of November 15, 2013) 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[31] and that she can license others next to Facebook (the license is non-exclusive)[32]. The question in this section is whether this general IP clause entails that Facebook's prior consent is required for the acts of reproduction (to a lesser

---

[28] **Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance)** OJ L 111, 5.5.2009, p. 16–22.

[29] The national copyright laws of the Member States of the EU may vary on this point. See Trialle et al. (2014), 585, 98-108.

[30] Online available at: <https://www.facebook.com/legal/terms>.

[31] The matter is more complicated where users share works to which they do not hold the copyright, such as pictures, news articles or videos.

[32] Such licences raise many legal questions on the relation between the user and the OSN. These will be addressed in D3.3.

extent distribution and communication to the public) performed for the construction of a transparency tool (absent an exception for data mining[33]).

We know that a user's Facebook profile may contain expressions protected under copyright, such as status updates or pictures she has made. Making a copy of such works (e.g. downloading them to your server in order to analyse them) is to *reproduce* the works, an act that requires the author's prior consent (i.e. the Facebook user's consent or even a third party where the Facebook user has "posted" works from another author)[34]) only allowed when the copyright holder has allowed you to do so ("given you a license").

Considering that the general IP clause in Facebook's general terms and conditions provides a non-exclusive licence, it could be argued that USEMP does not need Facebook's consent to process protected content from users (or third parties). In the USEMP Data License Agreement (see D3.1) signed by every USEMP user and the USEMP Consortium Partners, a license is given to the USEMP consortium to use all data gathered through the DataBait Facebook app and the browser plug-in for the specific purpose of USEMP research.

Considering that the IP licence is transferable and sub-licensable, Facebook's consent would however be sufficient (provided that the licence is valid in the first place). An interesting question is if, when no such direct agreement is signed with the author of copyrighted material, the IP license is implicitly provided by Facebook to app developers as a form of sublicensing. This question is not answered by the Art. 9 (*Special Provisions Applicable to Developers/Operators of Applications and Websites*) or Art.10 (*About Advertisements and Other Commercial Content Served or Enhanced by Facebook*) of the *Facebook Statement of Rights and Responsibilities*[35] (see the Annex for the full text of these two articles).

Art. 2 of the Facebook Statement of Rights and Responsibilities, however, does not provide a watertight solution for the cases where a Facebook user has posted protected subject matter created by another author to her profile, without this author's consent. Where such protected content is then processed in an automated way, the general consent clause vis-à-vis the Facebook user cannot provide a legal basis towards an author, who has not authorised her work being shared by the Facebook user in the first place. It may be necessary to include a warranty clause in the DLA, or develop a separate DLA regarding copyright issues. Also, Facebook's consent is required where protected elements of Facebook's creations are reproduced (e.g. graphic user interfaces, elements of the computer program).

In summary, an OSN may hold copyright on various aspects of the OSN. Firstly, there are the copyrights on its own creations (it can be assumed that these have been acquired from the creators such as employees or consultants), such as computer programs, interfaces and

---

[33] Trialle et al (2014),122
http://ec.europa.eu/internal_market/copyright/docs/studies/1403_study2_en.pdf.

[34] Unless such copies could be exempted under the exception of "temporary reproduction", but the list of conditions is rather strict: see Article 5 of the Copyright ("InfoSoc") Directive. Exceptions and limitations
1. Temporary acts of reproduction […], which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
(a) a transmission in a network between third parties by an intermediary, or
(b) a lawful use
of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

[35] Online available at : <https://www.facebook.com/legal/terms>.

perhaps also databases (see next section). Secondly, the OSN users post protected works (their own works or third party works, with or without consent). Facebook, for example, has provided a general IP clause in the form of a non-exclusive, transferable and sub-licensable licence. In D3.4 (and its successor, D3.9), it will be verified on the basis of the technical description of the DataBait tools (development and operation of the tools) which elements are processed and reproduced. For each element it should be verified (i) whether the consent of the right holder is required or if an exception applies (so no consent is required), (ii) who holds the exclusive rights and is authorised to consent (cf. D3.3 and D3.8) and (iii) whether such consent can be acquired (USEMP's data licence, Facebook's implicit licence, or an alternative solution).

2.5. Profiling and the IP protection of databases

Up until now we have focused on copyrighted content that is part of one's profile (a status update, a video, a picture, etc.). In addition, the profile as a whole could be the subject matter of another layer of intellectual property protection. The Member States of the European Union indeed provide protection for databases, following the adoption of the Database Directive (DBD)[36].

A database is defined as "a collection of independent works, data or other materials arranged in a systematic way or methodical way and individually accessible by electronic or other means" (Art. 1(2) DBD).

The DBD provides a two-tier protection for databases: the database may be protected under copyright (structure) or the "sui generis" protection on the content of the database.

Firstly, there may be **copyright** protection for databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation (Art. 3 DBD). It is important to underline that in such a case the copyright is not on the content of the database (one particular status update or one individual profile) but on its particular structure ("selection or arrangement"). The structure of the database can be protected under copyright provided that it meets the originality requirement, i.e. it is the author's own intellectual creation[37]. It is assumed that a profile (either the individual profile or a data model) that has been composed purely in an automated manner will not be protected by copyright (see e.g. Roosendaal, 2013).

Holding a copyright over the structure ("expression") of a database gives the author of the database the right to permit or prohibit reproduction, publication and distribution (Art. 5 of the Database Directive).

Article 5. Restricted acts

In respect of the expression of the database which is protectable by copyright, the author of a database shall have the exclusive right to carry out or to authorize:

(a) temporary or permanent reproduction by any means and in any form, in whole or in part;

[36] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases ("Database Directive"), *Official Journal* L 077, 27/03/1996 P. 0020 – 0028.
[37] CJEU, Football Dataco Ltd and Others v Yahoo! UK Ltd and Others, C-604/10, ECLI:EU:C:2012:115.

(b) translation, adaptation, arrangement and any other alteration;

(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;

(d) any communication, display or performance to the public;

(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).

Secondly, next to the classical copyright protection of databases, there is also a ***sui generis* database right** in favour of the maker of the database (art. 7 DBD). Such protection is available for databases provided that there has been qualitatively and/or quantitatively a substantial investment, either in the obtaining, or in the verification or the presentation of the contents. The investment in the creation of the content is not taken into account[38].

A substantial investment…

> "… may consist in the deployment of financial resources and/or the expending of time, effort and energy." (Recital 40 of the DBD)

Where a substantial investment in the obtaining, verification or presentation of the contents of the database can be demonstrated, the maker of the database has an exclusive right covering the extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database (art. 7 DBD). In the next version of the report, depending on the further development of USEMP tools, we may elaborate an analysis of these exclusive rights, based on cases decided by the CJEU on re-utilisation/extraction (e.g. Sportradar).

A database can simultaneously be protected by copyright (protecting the author from unauthorized reproduction, adaptation, communication and distribution of the database structure) and by the sui generis right (protecting the maker of the database from to unauthorized extraction and/or re-utilization of the whole or of a substantial part of the database).

The copyright and sui generis right on databases is of particular interest to the USEMP project – do profile transparency tools like the ones created by USEMP reproduce (parts) of the overall structured way in which data are organized by, for example, Facebook? After all, we cannot be sure that Facebook will not invoke exclusive database rights. Although Facebook does not invest in the creation or verification of the content of the database per se (this is added by the users), it arguably makes substantial efforts for the presentation of the content. It could also be argued that the structure of the database shows a certain degree of originality (cf. the subsequent changes to the presentation of the user's profiles, e.g "walls", "timelines", "newsfeeds"). In this case, it is not the Facebook user who decides what her profile looks like; she uses the mould defined by Facebook.

It will be verified in the next version of this deliverable whether, either during the creation or the operation of the DataBait tools, the database of the OSN is used in any way protected under copyright or the producer's database rights (extraction or re-utilisation / reproduction,

[38] See *inter alia* Fixtures Marketing Ltd v Oy Veikkaus Ab, C-46/02, ECLI:EU:C:2004:694 ; The British Horseracing Board Ltd and Others v William Hill Organization Ltd, C-203/02, ECLI:EU:C:2004:695.

distribution or communication to the public of elements). This will be done on the basis of the description of the activities of our technical partners.

In the case of the USEMP project the question whether the DataBait tools infringe on the copyright and sui generis right of commercial profilers might be (partly) resolved through the exceptions with regard to scientific research: reproduction (copyright) and extraction or re-utilization of substantial parts of a database (sui generis right) for the sole purpose of scientific research is likely[39] to fall under the exceptions in Art 6(2b) and Art. 9(b) of the Database Directive – at least when one interprets "providing the USEMP end-user with information about his or her profile" as "extraction for the purpose of illustration of scientific research".

Article 6 of the Database Directive

Exceptions to acts restricted by the copyright on a database

1. The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database. Where the lawful user is authorized to use only part of the database, this provision shall apply only to that part.

2. Member States shall have the option of providing for limitations on the rights set out in Article 5 in the following cases:

(a) in the case of reproduction for private purposes of a non-electronic database;

(b) where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;

(c) where there is use for the purposes of public security of for the purposes of an administrative or judicial procedure;

(d) where other exceptions to copyright which are traditionally authorized under national law are involved, without prejudice to points (a), (b) and (c).

Article 9 of the Database Directive

Exceptions to the sui generis right

Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents:

(a) in the case of extraction for private purposes of the contents of a non-electronic database;

(b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;

[39] See for a more nuanced and detailed discussion: Traille et al., 2014.

(c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

However, there are two caveats about the protection offered by the three aforementioned exceptions for scientific research.

Firstly, the exceptions are optional – not every Member State has opted to implement them in their national legislation[40]. Secondly, tools similar to the ones developed by USEMP which are used outside a purely scientific context will probably infringe on database rights. Consequently, verification is required to check whether in the case that under the applicable national law the conditions of the exceptions for the purpose of scientific research are not met, the USEMP Consortium needs the prior consent of the holder of the copyrights and the sui generis database rights (i.e. Facebook). Absent such prior consent, the USEMP Consortium could be vulnerable to claims of infringements to the intellectual rights covering the databases.

[40] Triaille e.a. (2014) studied the implementation of the scientific exceptions in the following member states : Netherlands, Germany, Poland, Luxembourg, Denmark, Hungary, Belgium, Spain, the UK and Italy. "The exception to copyright for scientific research in relation to databases contained in Article 6(2)(b) of the Database Directive has been implemented in four Member States among those considered in this Study: Belgium, Spain, the UK and Italy. […] Other Member States – the Netherlands, Germany, Poland, Luxembourg, Denmark and Hungary – have not implemented the exception for scientific research to the copyright protection of databases contained in Article 6(2)(b) of the Database Directive". (p. 68); “The exception to the sui generis right for scientific research contained in Article 9(b) of the Database Directive has been implemented in nine countries among those considered in this study: Belgium, Spain, the UK, the Netherlands, France, Germany, Poland, Luxembourg, and Hungary.” (p. 80); “Except for Spain and the Netherlands, the exception for scientific research contained in article 5(3) a) of the Infosoc Directive has been transposed in all the Member States that are analyzed by the Study" (p.53). This study did not concern Swedish law.

3. Conclusion and next steps

The conclusions are preliminary and depend on the current state of the USEMP project. At the moment of finalizing the text of D3.2 it is not entirely clear how exactly which data are processed, at whose premises and for what reasons. To elaborate on the issues at stake in this deliverable we need a more exhaustive overview of how the DataBait tools function, which elements are being copied, how long they are stored and for what purpose the protected subject matter will be used. Based on the previous analysis and the current state of DataBait tool development, we suggest the following research issues as highly relevant for the next version of this deliverable (D3.7), to be delivered in month 24 of the project.

(a) A further analysis of the tension between profile transparency and the IP rights of the actors performing tracking and profiling practices (such as OSNs, browsers and third-parties) and the possibility of providing profile transparency through tools such as the ones developed by USEMP.

Tensions arise with trade secrets on data models or training sets, copyrighted elements of profiles or databases (pictures, status updates, etc.), and the copyright and sui generis right on databases. To elaborate on this we need a more precise understanding of what data must be processed for what purpose, how and by which data controller, in order to provide adequate inferences on what data controllers may infer from the user's data. Inferring what others may infer is what has been called counter-profiling.

In line with the introductory chapter, this further analysis has a triple goal: (1) exploring the rights of commercial profilers to (partly) oppose claims to profile transparency, (2) make sure that the USEMP tools do not infringe on these IP rights of profilers when providing profile transparency to its end-users, (3) inform USEMP end-users through the DataBait graphic user interface about the possible tensions between IP rights of profilers and their right to profile transparency.

(b) A further analysis on the legal compatibility of the USEMP tools with IP rights of profilers, notably with those of the OSN provider.

(i) Once it has become more clear what which elements of OSNs are exactly processed by which of the USEMP Consortium Partners, and for what purpose, it will be possible to determine the legal compatibility of such processing with eventual IP rights of OSN/profilers. The following questions will be verified on the basis of the actual activities of the technical partners: (i) which subject matter is protected under which regime (trade secret, patent, copyright with different rules per type of subject matter); (ii) does USEMP perform any restricted act (in relation to protected elements) during the development or the operation of the DataBait tools; (iii) does any exception apply (taking into account that the tools are presently developed and used for the purpose of scientific research); (iv) have the USEMP partners acquired licences for their activities.

There are some exceptions for scientific research in the Copyright ("InfoSoc") and Database Directive. However, not every Member State

has implemented these exceptions. Legislation with regard to trade secrets is scattered but at the moment it seems unlikely that a Member State would offer a statutory exception with regard to infringements on trade secrets. It may be interesting, however, to also investigate whether individuals could base deployment of transparency tools on the need to provide effective tools to exercise freedom of information. It may also be useful to analyse the exception for temporary acts of reproduction in more detail.

(ii) Since USEMP investigates tools aimed to empower users of OSNs beyond the scope of a research setting, we will extend the research into an analysis of the legal compatibility with IP rights of profilers of the DataBait tools in a commercial market, as examples of Data Protection by Design, developed and provided by commercial or non-profit data controllers.

Since the exceptions for scientific research will not apply in that case, a further analysis is required into the extent to which such tools may violate copyright, sui generis database rights or trade secrets.

(iii) The USEMP partners face a particular challenge in complying with the various legal regimes, applicable to distinct aspects of the development or operation of the tools. The distinct IP rights (considering the lex specialis for databases and computer programs) cover different acts and provide different exceptions, which makes it complicated to comply with all provisions under all circumstances.

Finally, this legal research will have implications for the USEMP OSN Presence tool and the USEMP OSN Economic Value Awareness tool: while avoiding unnecessary legalese, succinct information on relevant IP rights of profilers should be included in the USEMP tools. For example, in the Economic Value Awareness tool one could inform users about the royalty-free license they have given to Facebook on all their copyright protected material, explaining the notion and implications of copyright.

Bibliography

Ateniese, G., Felici, G., Mancini, L. V., Spognardi, A., Villani, A., & Vitali, D. (2013). Hacking smart machines with smarter ones: how to extract meaningful data from machine learning classifiers. arXiv preprint arXiv:1306.4447.

Baker & MacKenzie, Study on trade secrets and confidential business information in the internal market, Study prepared for the European Commission by Baker & McKenzie, 2013, available at http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

Custers, B. (2009). Profiling in Financial Institutions. FIDIS (The Future of Identity in the Information Society) deliverable 7.16 (pp. 57-67). Brussels: EU.

Ferraris, V., Bosco, F., Cafiero, G., D'Angelo, E., & Suloyeva, Y. (2013). Defining Profiling. Working paper on definition and domain of application of profiling. Profiling. Protecting Citizens' Rights Fighting Illicit Profiling: Research Project funded by the European Commission, DG Justice, under the Fundamental Rights and Citizens programme.

Hildebrandt, M. (2008). Defining profiling: a new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), Profiling and the Identity of the European Citizen (pp. 39-50): Springer.

Holbrook, T.R. (2007). Extraterritoriality in US Patent Law, (4) William & Mary Law Review 6, 2119-2192.

Roosendaal, A. (2013). Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts [Ph.D. thesis, Tilburg University]. Oisterwijk: Wolf Legal Publishers.

Triaille, J.-P., de Meeûs d'Argenteuil, J., & de Francquen, A. (2014). Study on the legal framework of text and data mining (TDM). Brussels: European Union.

Van Dijk, N. (2009). Intellectual Rights as Obstacles for the Transparency of Profiling Processes. In A. Deuker (Ed.), From Mobile Marketing in the Perspective of Identity, Privacy and Transparency, FIDIS deliverable 11.12 (pp. 57-67).

van Dijk, N. (2010a). Auteursrecht in profielen. Computerrecht, 35(2), 53 - 61.

Van Dijk, N. (2010b). Property, Privacy & Personhood in a World of Ambient Intelligence. Ethics and Information Technology, 12(1), 57 - 69.

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

Case Law

Ashby Donald and others v. France, Appl. nr. 36769/08, ECtHR (5th section), Strasbourg 10 January 2013 ;

Fixtures Marketing Ltd v Oy Veikkaus Ab, C-46/02, ECLI:EU:C:2004:694 ;

The British Horseracing Board Ltd and Others v William Hill Organization Ltd, C-203/02, ECLI:EU:C:2004:695.

Infopaq International A/S v Danske Dagblades Forening, C-5/08, ECLI:EU:C:2009:465, para. 37.

Eva-Maria Painer v Standard VerlagsGmbH and Others, C-145/10, ECLI:EU:C:2011:798

Football Dataco Ltd and Others v Yahoo! UK Ltd and Others, C-604/10, ECLI:EU:C:2012:115.

Deckmyn v. Vandersteen, C-201/13, EU:C:2014:2132.

Annex A

From the *Facebook Statement of Rights and Responsibilities*[41] (version of November 15, 2013):

Art. 9. Special Provisions Applicable to Developers/Operators of Applications and Websites

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Facebook Platform Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
    1. You will only request data you need to operate your application.
    2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.
    3. You will not use, display, share, or transfer a user's data in a manner inconsistent with your privacy policy.
    4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
    5. You will not include data you receive from us concerning a user in any advertising creative.
    6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
    7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
    8. We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.

[41] Online available at: <https://www.facebook.com/legal/terms>.

9. We can limit your access to data.
10. You will comply with all other restrictions contained in our Facebook Platform Policies.

3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on www.facebook.com.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Facebook Platform Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
    1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
    2. comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, timelines, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

Art. 10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.