



# SPION

## From social media service to advertising network

*A critical analysis of Facebook's Revised Policies and Terms*

*DRAFT 25 August 2015*

v1.3



## About the authors

This report has been prepared by Brendan Van Alsenoy, Valerie Verdoodt, Rob Heyman, Jef Ausloos, Ellen Wauters and Güneş Acar.

It was written under the academic guidance of Prof. Dr. Peggy Valcke, Prof. Dr. Jo Pierson, Dr. Els Kindt, Prof. Dr. Eva Lievens, Prof. Dr. Marie-Christine Janssens, Prof. Dr. Claudia Diaz and Prof. Dr. Bart Preneel.

The authors are part of the Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights (ICRI/CIR) of KU Leuven ([www.icri.be](http://www.icri.be)), the department of Studies on Media, Information and Telecommunication (SMIT) of the Vrije Universiteit Brussel (VUB) ([www.smit.vub.ac.be](http://www.smit.vub.ac.be)) and the department of Computer Security and Industrial Cryptography (COSIC) of KU Leuven ([www.esat.kuleuven.be/cosic](http://www.esat.kuleuven.be/cosic)). All three departments are part of iMinds ([www.iminds.be](http://www.iminds.be)).

## Preface

This report has been commissioned by the Belgian Privacy Commission ([www.privacycommission.be](http://www.privacycommission.be)). The findings it contains build on the results of two research projects, namely EMSOC ([www.emsoc.be](http://www.emsoc.be)) and SPION ([www.spion.me](http://www.spion.me)). Both EMSOC and SPION were funded by the Flemish Agency for Innovation through Science and Technology ([www.iwt.be](http://www.iwt.be)).

The findings and views expressed in this report are solely those of the authors and should not be attributed to any of the other aforementioned entities.

The present report should be considered as **provisional** and will be updated after further research, deliberation and commentary. Comments and suggestions are welcome at [facebook.icri-cir@law.kuleuven.be](mailto:facebook.icri-cir@law.kuleuven.be).

## Version history

No.	Date	Version	Affected chapters	State
1	30/01/2015	1.0	ALL	Internal draft
2	23/02/2015	1.1	ALL	Public draft
3	31/03/2015	1.2	3, 4, 8	Public draft
4	25/08/2015	1.3	3, 4, 5, 6, 10	Public draft

<b>PREFACE .....</b>	<b>2</b>
<b>LIST OF ABBREVIATIONS .....</b>	<b>7</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>1. INTRODUCTION .....</b>	<b>10</b>
A. HORIZONTAL EXPANSION .....	10
B. VERTICAL EXPANSION .....	10
C. GENERAL ASSESSMENT OF THE REVISED TERMS .....	11
<b>2. CONSENT .....</b>	<b>12</b>
A. ROLE OF CONSENT .....	12
B. REQUIREMENTS FOR VALID CONSENT .....	13
1) <i>Indication of wishes</i> .....	14
2) <i>Freely Given</i> .....	14
3) <i>Specific</i> .....	15
4) <i>Informed</i> .....	16
5) <i>Unambiguous</i> .....	17
<b>3. PRIVACY SETTINGS .....</b>	<b>18</b>
A. SOCIAL PRIVACY SETTINGS .....	20
1) <i>Posts</i> .....	20
2) <i>Contact and Basic Info</i> .....	21
3) <i>“Public Information” and “Public Profile”</i> .....	24
4) <i>Search engines</i> .....	24
5) <i>“Friend list” and “Following”</i> .....	27
6) <i>“Timeline” and “Tagging”</i> .....	28
B. APPLICATION SETTINGS .....	31
1) <i>Applications which users download themselves</i> .....	31
2) <i>Applications downloaded by friends</i> .....	35
3) <i>Platform setting</i> .....	36
4) <i>Play anonymously</i> .....	37
C. ADVERTISING SETTINGS .....	38
1) <i>Ads and Friends</i> .....	38
2) <i>Behavioural advertising</i> .....	39
D. ASSESSMENT .....	40
1) <i>False sense of control</i> .....	40
2) <i>Inconsistent definitions</i> .....	41
3) <i>Insufficient control over indexation</i> .....	41
4) <i>Insufficient tag controls</i> .....	41
5) <i>Apps downloaded by friends</i> .....	42
6) <i>Complex opt-out mechanisms</i> .....	43
<b>4. UNFAIR CONTRACT TERMS .....</b>	<b>45</b>
A. EXCESSIVE LINKING .....	45
B. CHARACTERISATION AS A “FREE” SERVICE .....	47
C. WARRANTY DISCLAIMER .....	48

D.	LIABILITY LIMITATION .....	48
E.	INDEMNITY CLAUSE .....	49
F.	UNILATERAL CHANGE .....	50
G.	FORUM CLAUSE .....	51
H.	CHOICE OF LAW .....	53
I.	TERMINATION .....	53
<b>5.</b>	<b>HOW FACEBOOK “COMBINES” AND “SHARES” DATA ABOUT ITS USERS .....</b>	<b>55</b>
A.	CUSTOM AUDIENCES .....	55
1)	<i>Customer List</i> .....	56
2)	<i>Website traffic</i> .....	58
3)	<i>App activity</i> .....	60
4)	<i>Additional Facebook targeting options</i> .....	61
B.	LOOKALIKE AUDIENCES .....	63
C.	ATLAS .....	65
D.	ASSESSMENT .....	67
1)	<i>Non-restrictive language</i> .....	68
2)	<i>Catch-all provisions</i> .....	69
3)	<i>Sources and recipients of data</i> .....	69
4)	<i>Inadequate user controls</i> .....	71
<b>6.</b>	<b>LOCATION DATA .....</b>	<b>73</b>
A.	FACEBOOK’S 2013 DUP .....	74
B.	FACEBOOK’S 2015 DUP .....	74
C.	ASSESSMENT .....	75
<b>7.</b>	<b>FURTHER USE OF USER-GENERATED CONTENT .....</b>	<b>76</b>
A.	FACEBOOK’S IP LICENSE .....	76
B.	“SPONSORED STORIES” AND “SOCIAL ADS” .....	81
1)	<i>Unsolicited communications</i> .....	83
2)	<i>Identifying commercial communications</i> .....	84
3)	<i>Right to control the use of one’s image</i> .....	86
<b>8.</b>	<b>TRACKING THROUGH SOCIAL PLUG-INS .....</b>	<b>89</b>
A.	TRACKING OF USERS AND NON-USERS .....	89
B.	FACEBOOK AUDITS 2011-2012 .....	90
1)	<i>The 2011 Report of Audit</i> .....	90
2)	<i>The 2012 Report of Re-Audit</i> .....	91
C.	FACEBOOK’S 2013 DUP .....	92
D.	FACEBOOK’S 2015 DUP .....	93
E.	ASSESSMENT .....	94
1)	<i>Article 5(3) of the e-Privacy Directive</i> .....	94
2)	<i>Position of the Article 29 Working Party</i> .....	95
3)	<i>Facebook’s tracking of users</i> .....	96
4)	<i>Facebook’s tracking of non-users</i> .....	97
5)	<i>Facebook’s proposed opt-out mechanism</i> .....	98
6)	<i>Alternatives</i> .....	99
<b>9.</b>	<b>FINGERPRINTING .....</b>	<b>100</b>

A.	FACEBOOK’S 2013 DUP .....	100
B.	FACEBOOK’S 2015 DUP .....	101
C.	ASSESSMENT .....	102
<b>10.</b>	<b>DATA SUBJECT RIGHTS .....</b>	<b>103</b>
A.	RIGHT TO INFORMATION .....	103
1)	<i>Identity of the controller</i> .....	103
2)	<i>Purposes of the processing</i> .....	103
3)	<i>Recipients or categories of recipients</i> .....	104
4)	<i>Categories of data</i> .....	104
5)	<i>Data subject rights</i> .....	105
B.	RIGHT OF ACCESS.....	105
C.	RIGHTS TO OBJECT AND ERASURE .....	107
1)	<i>Right to object</i> .....	107
2)	<i>Right to erasure</i> .....	108

## List of abbreviations

CJEU	Court of Justice of the European Union
DUP	Data Use Policy
OSN	Online Social Network
SSR	Statement of Rights and Responsibilities
WP29	Article 29 Data Protection Working Party

## **Executive summary**

### **1. CONSENT**

Data subject consent is the only viable justification for many of Facebook's processing activities. To be valid, consent must be "freely given", "specific", "informed" and "unambiguous". Given the limited information Facebook provides and the absence of meaningful choice with regard to certain processing operations, it is highly questionable whether Facebook's current approach satisfies these requirements.

### **2. PRIVACY SETTINGS**

Facebook has not announced any changes to its privacy settings as part of the 2015 changes. Nevertheless, its current default settings with regards to behavioural profiling and advertising (essentially "opt-out") remain problematic. According to the Article 29 Working Party, consent cannot be inferred from the data subject's inaction with regard to behavioural marketing. As a result, Facebook's opt-out system for advertising does not meet the requirements for legally valid consent. In addition, opt-outs for "Sponsored Stories" or the collection of location data are simply not provided.

### **3. UNFAIR CONTRACT TERMS**

In comparison to 2013, Facebook's new Statement of Rights and Responsibilities (SRR) has not changed substantially. However, our analysis shows that there are several clauses which violate European consumer protection law. Specifically, Facebook's SRR contains a number of provisions which do not comply with the Unfair Contract Terms Directive. These violations were already present in 2013, and they are set to persist in 2015.

### **4. HOW FACEBOOK "COMBINES" AND "SHARES" DATA ABOUT ITS USERS**

Facebook can combine data from an increasingly wide variety of sources (e.g., Instagram, Whatsapp and data brokers). By combining information from these sources, Facebook gains a deeper and more detailed profile of its users. Facebook only offers an opt-out system for its users in relation to profiling for third-party advertising purposes. The current practice does not meet the requirements for legally valid consent.



## **5. FURTHER USE OF USER-GENERATED CONTENT**

Facebook's terms allow the company to use user-generated content (e.g., photos) for commercial purposes (e.g., Sponsored Stories, Social Ads). While the revised terms communicate this practice in a more transparent way, Facebook fails to offer adequate control mechanisms. In addition, the actual use of user-generated content in commercial communications is not transparent at all. Users might be aware of the possibility that their content might appear in ads, but they are kept unaware about when and how this actually happens.

## **6. LOCATION**

Facebook collects location data from a variety of sources. The only way to stop the Facebook mobile app from accessing location data on one's smartphone is to do so at the level of the mobile operating system. Facebook should provide more granular ("in app") location-data settings, with all parameters turned off by default. These settings should allow users to determine when and how location data can be used by Facebook and to what purpose.

## **7. TRACKING**

Facebook monitors its users in a variety of ways, both off and on Facebook. While Facebook provides users with high-level information about its tracking practices, we argue that the collection or use of device information envisaged by the 2015 DUP does not comply with the requirements of article 5(3) of the e-Privacy Directive, which requires free and informed prior consent before storing or accessing information on an individual's device. Facebook also tracks non-users in a manner which violates article 5(3) of the e-Privacy Directive.

## **8. DATA SUBJECT RIGHTS**

Facebook's terms do not properly acknowledge the data subject rights of its users. While Facebook offers certain voluntary transparency tools, none of these tools provide a complete overview of all data collected, nor do they make explicit the actual purposes for which personal data have been used. In addition, users may easily be misled into thinking that their right to erasure only extends to self-posted content or requires full account deletion.

# 1. Introduction

Facebook's revised Data Use Policy (DUP) is an extension of existing practices. This nevertheless raises concerns because Facebook's data processing capabilities have increased both horizontally and vertically. By horizontal we refer to the increase of data gathered from different sources. Vertical refers to the deeper and more detailed view Facebook has on its users. Both are leveraged to create a **vast advertising network** which uses data from inside and outside Facebook to target both users and non-users of Facebook.

## A. Horizontal expansion

Facebook combines data from an **increasingly wide variety of sources**. These sources include acquired companies, partnering platforms and websites or mobile applications that rely on Facebook (or one of its companies) for advertising or other services. In addition, Facebook's ability to monitor and track users' activities outside Facebook has increased exponentially as time has gone by. Facebook's tracking capabilities have expanded mainly through the spread of social-plugins ("like buttons")<sup>1</sup> and through new forms of mobile tracking.

## B. Vertical expansion

Vertical expansion refers to the **growing variety of types of information** that are obtained regarding Facebook users. Through the acquisition of Instagram and WhatsApp, but also by adding new functionalities, Facebook is able to collect more types of user data. These new data types enable more detailed profiling.

Under Facebook's DUP, **data usage is not limited to one or more clearly defined purposes**. If data is collected in order to improve the service for the user, for example the same data can also be used for advertising purposes. Location data is a clear example: Facebook collects location data in order to allow users to share their location with peers. However, this data may also be re-used to target advertising.

---

<sup>1</sup> Social-plugins were initially introduced to allow individuals to show their appreciation for specific content (a user-oriented goal). Facebook now gathers information through these buttons and plugins regardless of whether these buttons are actually used.

### **C. General assessment of the revised terms**

Overall, Facebook's revised DUP signals the company's data use practices in a more prominent way. In this regard, Facebook seems to have taken an important step forward. However, the uses of data are still only communicated on a general and abstract level. Much of the DUP consists of hypothetical and vague language rather than clear statements regarding the actual use of data. Moreover, the choices Facebook offers to its users are limited. For many data uses, the only choice for users is to simply "take-it-or-leave-it". If they do not accept, they can no longer use Facebook and may miss out on content exclusively shared on this platform. In other words, Facebook leverages its dominant position on the online social network (OSN) market to legitimise the tracking of individuals' behaviour across services and devices.

The re-use of user content for targeting and advertising purposes is deeply embedded in Facebook's practices. It is impossible to add any information that may not later be re-used for targeting, and any "like" may become a trigger to portray a user in a "Sponsored Story" or "Social Ad". From the latter one can opt-out, but the only way to stop appearing in Sponsored Stories, is by stopping to "like" content altogether. Users are even more disempowered because they are unaware about how exactly their data is used for advertising purposes. Furthermore, they are left in the dark about their appearance in promotional content. Facebook should not only provide users with more options to control how their data is gathered, but also show users how their name and picture is used in specific instances.

## 2. Consent

### A. Role of consent

Under Directive 95/46/EC<sup>2</sup>, processing of personal data may only take place to the extent that there is a **“legitimate ground”** justifying the processing. The legitimate grounds recognised by the Directive are enumerated (exhaustively) in article 7. Of these grounds, there are **three grounds** in particular which the provider of an OSN might invoke, namely:

- the unambiguous consent by the data subject<sup>3</sup>;
- a necessity for the performance of a contract<sup>4</sup>; and
- an (overriding) legitimate interest<sup>5</sup>.

For processing that is **strictly necessary to provide the OSN service** (e.g., initial creation of profile, offering of basic functionalities), the OSN provider can in principle rely on the ground of “necessity for the performance of a contract”.<sup>6</sup> For a limited number of operations, the provider may also be able to rely on the **“legitimate interest”** ground (e.g., processing for purposes of ensuring system security).<sup>7</sup> For all other processing operations, such as the use of users’ personal data for targeting purposes, the provider will in principle have to obtain the **“unambiguous consent”** of its users.<sup>8</sup>

There are **situations in which data subject consent is mandated** by law, even if the controller might theoretically be able to invoke another ground to legitimise the processing. For instance, **article 5(3) of the E-Privacy Directive**<sup>9</sup> entails that OSN providers must obtain the consent of its users prior to:

---

<sup>2</sup> Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, *O.J.*, L-281, 23 November 1995, 31-50. Hereafter also referred to as ‘Directive 95/46’ or simply ‘the Directive’. In Belgium, Directive 95/46 was implemented by modifying the Belgian Law of 8 December 1992 on privacy protection in relation to the processing of personal data (*B.S.*, 18 March 1993) (hereafter the “Belgian Data Protection Act” or “BDPA”).

<sup>3</sup> Article 7(a) Directive 95/46; article 5(a) BDPA.

<sup>4</sup> Article 7(b) Directive 95/46; article 5(b) BDPA.

<sup>5</sup> Article 7(f) Directive 95/46; article 5(f) BDPA.

<sup>6</sup> P. Van Eecke and M. Truyens, ‘Privacy and Social Networks’, *Computer Law & Security Review* 2010, Vol. 26, p. 537-538

<sup>7</sup> *Idem.*

<sup>8</sup> For a more detailed analysis on the role of consent as a basis for legitimating the processing of personal data see B. Van Alsenoy, E. Kosta and J. Dumortier, “Privacy notices versus informational self-determination: Minding the gap”, *International Review of Law, Computers & Technology* 2013, and the references provided there .

<sup>9</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L-201, 31 July 2002, 37-47, as amended by Directive 2009/136/EC of the European

- the installation of any software on the device of an end-user (e.g., when offering a mobile application for the OSN);
- any placement of cookies which are not strictly necessary to provide service (e.g., to monitor web-browsing activities outside the OSN).<sup>10</sup>

Article 5(3) of the e-Privacy Directive is particularly relevant in relation to the **tracking** techniques used by certain OSN providers, including Facebook (cf. *infra*; section 8 “Tracking through social plug-ins”).

As far as the use of OSN data for purposes of **targeted advertising** is concerned, the situation is somewhat less clear-cut. Directive 95/46 does not explicitly state that individuals must provide consent before their data is used for purposes of direct marketing or targeted advertising. As a result, one might argue that the use of profile information of OSN users (e.g., name, age, location, etc.) for purposes of targeted advertising does not necessitate consent. However, even in absence of a legal provision mandating consent, a normal reading of article 7 of Directive 95/46 *de facto* requires users’ consent in order to legitimate these types of processing activities.<sup>11</sup> The same arguably applies for any processing of data intending to locate the **geographic position** of the end-user, regardless of whether it involves any storage of information on the device of the end-user.<sup>12</sup>

## B. Requirements for valid consent

Pursuant to article 2(h) of Directive 95/46, consent needs to be “**freely given**”, “**specific**”, “**informed**”, and “**unambiguous**” (or “explicit”) in order to be valid.<sup>13</sup> Where processing is based on consent, individuals in principle also have the right to withdraw consent and to see the underlying personal data removed.<sup>14</sup>

---

Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *O.J. L-337*, 18 December 2009. 11-36. Article 5(3) of the e-Privacy Directive has implemented in Belgian law by way of article 129 of the (revised) Law of 13 June 2005 concerning electronic communication (B.S., 20 June 2006).

<sup>10</sup> See also B. Van Alsenoy, “Rights and obligations of actors in social networking sites”, SPION D6.2, 2014, v1.2, p. 33-34 and 38, accessible at [www.spion.me](http://www.spion.me).

<sup>11</sup> See also E. Kosta, *Consent in European Data Protection Law*, 2013, Martinus Nijhoff Publishing, Leiden, p. 188-202, discussing “the erroneous debate around “opt-in” and “opt-out” consent.

<sup>12</sup> See also Article 29 Data Protection Working Party, “Opinion 13/2011 on Geolocation services on smart mobile devices”, WP185, 16 May 2011, p. 14.

<sup>13</sup> Article 29 Data Protection Working Party, “Opinion 15/2011 on the definition of consent”, WP187, 25 November 2011. See also article 1(8) BDPA.

<sup>14</sup> Article 29 Data Protection Working Party, “Opinion 2/2010 on online behavioural advertising”, WP171, 22 June 2010, p. 17.

## 1) Indication of wishes

When registering with Facebook for the first time, individuals actively need to click the button “Sign Up”, below the following text

*“By clicking Sign Up, you agree to our [Terms](#) and that you have read our [Data Use Policy](#), including our [Cookie Use](#).”*

According to WP29, the act of clicking might be considered to “signal, sufficiently clear to be capable of indicating a data subject’s wishes, and to be understandable by the data controller.”<sup>15</sup> To be valid, however, the data subject’s consent must also fulfil the following criteria:

## 2) Freely Given

Data subjects must have the ability to exercise “real choice”. There can be

*“no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.”<sup>16</sup>*

In practice, there are two elements that undermine an individual's ability to provide consent “freely” to Facebook's DUP. The first reason relates to the dominant position Facebook assumes on the OSN market. One of the primary reasons for joining is the fact that “everyone is on it”. Secondly, individual’s ability to withhold consent is constrained by Facebook’s “all-or-nothing” approach for many data uses. It is not possible, for example, to consent only to the basic OSN features, while not consenting to the use of one’s data for commercial profiling.<sup>17</sup> This practice goes against what the Article 29 Working Party has stated in its Opinion on Consent:

*“Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service. A pop-up box could be used to offer the user such a possibility.”<sup>18</sup>*

Finally, it is worth noting that the 2015 DUP explicitly extends “consent” to all of Facebook’s partner services (“Facebook Services”). By taking this approach, Facebook effectively leverages

---

<sup>15</sup> Article 29 Working Party, Opinion 15/2011 on the definition of consent”, *l.c.*, p. 11.

<sup>16</sup> *Ibid*, p. 12-13.

<sup>17</sup> Generally speaking, a distinction should be made between “requiring” and “requesting” information. See also House of Commons Science and Technology Committee, “Responsible use of data”, Fourth Report of Session 2014-15, 19 November 2014, p. 24-25, accessible at <http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf>

<sup>18</sup> Article 29 Working Party, Opinion 15/2011 on the definition of consent”, *l.c.*, p. 18.

its strong position as an OSN to legitimise the tracking and profiling of individuals' behaviour across services and devices.<sup>19</sup>

### 3) Specific

In order to be valid, a data subject's consent must relate to clearly identified data and purposes.<sup>20</sup> Put differently, the data subject's consent must be clearly and unambiguously given for a specific (category of) purpose(s).<sup>21</sup> Facebook's updated (and previous) DUP clearly lacks such specificity, both with regard to the data it collects as well as with regard to how it uses this data. It only identifies certain vague categories of purposes (e.g. "Provide, Improve and Develop Services"; "Promote Safety and Security"; "Show and Measure Ads and Services"), without providing a full and comprehensive list.

A few examples from the 2015 DUP:

- *"We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information."*
- *"We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friends tag you in a picture by comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged."*

Facebook does inform users of the categories of data that are shared when connecting one's account to an app on the "Facebook-Platform". It is unclear, however, to what extent user data is shared with other entities such as "service providers", "third-party partners" and "customers", nor what the exact identity is of these entities.<sup>22</sup> This issue has already been stressed in the WP29 Opinion on Consent:

*"Considering that the application can run without it being necessary that any data is transferred to the developer of the application, the WP encourages granularity while obtaining the consent of the user, i.e. obtaining separate consent from the user for the transmission of his data to the developer for these various purposes. Different mechanisms, such as pop-up boxes, could be used to offer the user the possibility to select the use of data*

---

<sup>19</sup> In its 2015 Cookie Policy, for example, Facebook stipulates "*Technologies like cookies, pixel tags ("pixels"), device or other identifiers and local storage (collectively, "Cookies and similar technologies") are used to deliver, secure, and understand products, services, and ads, on and off the Facebook Services."*

<sup>20</sup> Article 29 Working Party, Opinion 15/2011 on the definition of consent", *l.c.*, p. 17 et seq.

<sup>21</sup> See also the Opinion of Advocate General Sharpston delivered on 17 June 2010, Volker und Markus Schecke GbR, in Joined Cases C-92/09 and C-93/09: "*Acknowledging prior notice that publication of some kind will happen is not the same as giving 'unambiguous' consent to a particular kind of detailed publication.*" For more information see Article 29 Working Party, Opinion 15/2011 on the definition of consent", *l.c.*, p. 21-25.

<sup>22</sup> For a more detailed analysis cf. *infra*; Chapter 5 "How Facebook 'combines' and 'shares' information about its users".

*to which he agrees (transfer to the developer; added value services; behavioural advertising; transfer to third parties; etc.).”<sup>23</sup>*

#### 4) Informed

*“[T]here must always be information before there can be consent”.*<sup>24</sup> Research has shown<sup>25</sup> that individuals rarely read privacy notices or general terms of use, let alone understand them.<sup>26</sup> Merely providing a hyperlink - without requiring users to read the full text - has also been ruled insufficient by the CJEU in a consumer protection case.<sup>27</sup>

For consent to be “informed” under data protection law, the subject must be able to “appreciate and understand the facts and implications of his/her action”.<sup>28</sup> In principle, the data subject must be informed at least about:

- the identity of the controller and of his representative, if any;
- the purposes of the processing for which the data are intended;
- any further information such as
  - the recipients or categories of recipients of the data,
  - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  - the existence of the right of access to and the right to rectify the data concerning him.<sup>29</sup>

As mentioned earlier (cf. *supra*, specificity), Facebook fails to define the purposes for which the data will be processed in a comprehensive and intelligible fashion. The same applies with regard to its description of the (categories of) recipients of the data.

As to the presentation of the DUP, a lot can be learned from the WP29’s 2014 Letter regarding Google’s Privacy Policy.<sup>30</sup> According to its annex, the privacy policy should be immediately visible and accessible. It should contain an exhaustive list of all types of data as well as purposes for which it will be processed. Language such as “we can...” and “we may...” must be avoided.

---

<sup>23</sup> Article 29 Working Party, “Opinion 15/2011 on the definition of consent”, *l.c.*, p. 19. See also *infra*; section 5.D.

<sup>24</sup> Article 29 Working Party, “Opinion 15/2011 on the definition of consent”, *l.c.*, p.19.

<sup>25</sup> For an overview see E. Wauters, V. Donoso, E. Lievens and P. Valcke, “Re-designing & re-modeling Social Network terms, policies, community guidelines and charters: Towards a user-centric approach”, EMSOC D1.2.5, 31 March 2014, accessible at [www.emsoc.be](http://www.emsoc.be)

<sup>26</sup> See also House of Commons, Science and Technology Committee, Responsible Use of Data, *l.c.*, p. 18 et seq (“As a mechanism for showing that users have provided informed consent, so that organisations can process incredibly personal data, terms and conditions contracts are simply not fit for purpose.”)

<sup>27</sup> CJEU, *Content Services Ltd v Bundesarbeitskammer*, Case C-49/11 [2012]. See E. Wauters, E. Lievens and P. Valcke, “A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: ‘Rights & obligations in a social media environment’”, EMSOC D1.2.4, 19 December 2013, accessible at [www.emsoc.be](http://www.emsoc.be).

<sup>28</sup> Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131, 15 February 2007, p. 9.

<sup>29</sup> See also *infra*; section 10 A (“The Right to Information”)

<sup>30</sup> Article 29 Data Protection Working Party, Letter from the Article 29 Working Party to Google on Google Privacy Policy, 23 September 2014, accessible at [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index\\_en.htm#2014](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm#2014).



## 5) Unambiguous

“Unambiguous” means that the action by the data subject can *only* be understood as an expression of his/her agreement that personal data relating to him/her will be processed.<sup>31</sup>

Default settings which are configured to disclose information without the active engagement of the user do not constitute unambiguous consent.<sup>32</sup> When certain settings - not crucial to use the service - “overshare” data by default (e.g., with friends-of-friends or third party application providers), users are required to take active steps to undo this. It is questionable, according to WP29, “*whether not clicking on the button means that individuals at large are consenting.*”<sup>33</sup>

Facebook’s 2015 DUP provides that:

*“We use the [information we have](#) to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services. [Learn more](#) about advertising on our Services and how you can [control](#) how information about you is used to personalize the ads you see.”*

As discussed in the next chapter, it is highly questionable whether the manner in which controls are currently provided to users comply with either the requirement of “unambiguous” or “explicit” consent. As emphasised by the Article 29 Working Party, an opt-out mechanism “*is not an adequate mechanism to obtain average users informed consent*”, particularly with regard to behavioural advertising.<sup>34</sup> In other words, **Facebook’s opt-out approach with regard to behavioural profiling for advertising purposes does not meet the requirements for legally valid consent.**

---

<sup>31</sup> D. De Bot, *Verwerking van Persoonsgegevens* [‘Processing of Personal Data’], Kluwer, Antwerpen, 2001, p. 129. Where special categories of data are involved, article 8(2)a of the Directive specifies that the consent of the data subject must be “explicit” rather than “unambiguous”. The distinction between explicit and unambiguous is a subtle one, which is not always perceptible in practice. The main difference is that ‘absence of ambiguity’ still allows for inference from other (affirmative) actions, whereas ‘express’ consent does not allow for inference of any kind.

<sup>32</sup> See E. Kosta, *Consent in European Data Protection Law*, o.c., p. 200, discussing “the erroneous debate around “opt-in” and “opt-out” consent

<sup>33</sup> Article 29 Working Party, “Opinion 15/2011 on the definition of consent”, l.c., p. 24.

<sup>34</sup> Article 29 Working Party Opinion 2/2010 on online behavioural advertising, l.c., p. 15.

### 3. Privacy settings

Privacy settings are **access control mechanisms** that allow users to decide, to a certain extent, who can access their profile information and other content they share.<sup>35</sup>

Facebook **has changed its privacy settings many times**. In 2007, for example, Facebook introduced a new advertising feature (“Facebook Beacon”), which sent news alerts to users’ friends about the goods and services they buy and view on third-party websites (e.g., Blockbuster, Overstock.com).<sup>36</sup> There was fierce opposition to this service because it functioned on an opt-out basis, meaning that users had to take active steps to prevent other people from finding out about their off-Facebook activities.<sup>37</sup> In 2008, a class action suit was filed against Facebook<sup>38</sup> and in 2009 Facebook announced that it would stop the service.<sup>39</sup> In 2009, the default settings changed again, resulting in an increase of the data made publicly available by default.<sup>40</sup> In October 2013, Facebook changed its default settings for teenagers (aged 13-17).<sup>41</sup>

Facebook has **not announced any changes to the privacy settings for 2015**. Facebook did introduce “*Privacy Basics*”, which is an interactive tutorial to demonstrate how users can control access to their information. Interestingly, the “*Privacy Basics*” tutorial only informs users about “social” privacy controls, i.e. controls in relation to what other users can see or do. It does not walk users through the settings vis-à-vis advertising or access by third-party application providers.

---

<sup>35</sup> An ACM is the formalisation of how policies are composed based on a specific set of features in the system, regulating and authorising access to data. (R. Sayaf & D. Clarke, “Access Control Models For Online Social Networks”, 2, in L. Cavaglione et al. (eds), IGI Global, 2012 accessible at <https://lirias.kuleuven.be/bitstream/123456789/373507/1/ACMs%20in%20OSNs.pdf>).

<sup>36</sup> D. Boyd, E. Hargittai, “Facebook privacy settings: Who cares?”, *First Monday* vol. 15 n°8, 2 August 2010, accessible at <http://firstmonday.org/article/view/3086/2589#author>.

<sup>37</sup> C. Metz, *Facebook turns out light on Beacon*, 23 September 2009, [http://www.theregister.co.uk/2009/09/23/facebook\\_beacon\\_dies/](http://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/).

<sup>38</sup> N. Gohring, *Facebook faces class-action suit over Beacon*, 13 August 2008, <http://www.networkworld.com/news/2008/081308-facebook-faces-class-action-suit-over.html>.

<sup>39</sup> C. Metz, *idem*.

<sup>40</sup> A. Kuczerawy and F. Coudert, ‘Privacy Settings in Social Networking Sites: Is It Fair?’, in S. Fischer-Hübner et al. (Eds.): *Privacy and Identity Management for Life 6th IFIP AICT 352* (Springer, Heidelberg, 2011) 235.

<sup>41</sup> Facebook, *Teens Now Start With “Friends” Privacy for New Accounts; Adding the Option to Share Publicly*, 16 October 2013, <http://newsroom.fb.com/news/2013/10/teens-now-start-with-friends-privacy-for-new-accounts-adding-the-option-to-share-publicly/>.

# You're in charge.

We're here to help you get the experience you want. Learn about ways to protect your privacy on Facebook.

- > [What Others See About You](#)
- > [How Others Interact With You](#)
- > [What You See](#)

[Read our Data Policy](#)

Although no changes have been made to Facebook's default settings, the **default configurations** of certain settings **remain problematic**. The following sections will analyse three of the main settings available to Facebook users, namely:

- (A) Social privacy settings;
- (B) Application settings and;
- (C) Advertising settings.

## A. Social privacy settings<sup>42</sup>

### 1) Posts

Under the section “Privacy Settings and Tools”, Facebook provides several settings which allow users to restrict access to content which they post on Facebook. The default setting for “future posts” is set to “Friends” (for new users<sup>43</sup>). Other possibilities are “Public”<sup>44</sup>, “Friends of friends”, “Custom” and “Only me”.

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	No	Edit

In addition, users are able to define the audience for each post separately. When new users post something for the first time, they will be asked to select their audience for that particular post. If they don't select anything, their post will be shared with Friends only. If they do change the audience for that post, for instance to public, this change will remain, which means that future posts will also be shared publicly.<sup>45</sup>

<sup>42</sup> By “social privacy settings” we refer to settings that limit access by other Facebook users and non-users (ordinary internet users).

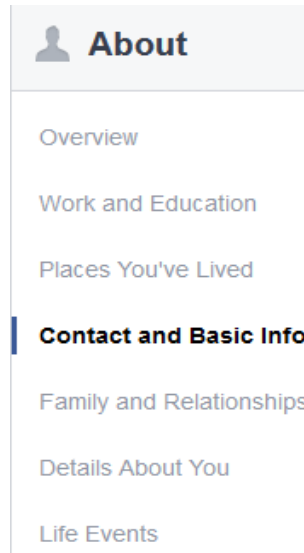
<sup>43</sup> For existing users the default setting used to be “public”.

<sup>44</sup> Public information can be seen by anyone, including “*people who aren't your friends, people off of Facebook and people who use different media such as print, broadcast (ex: television) and other sites on the Internet.*” See Facebook, “What is public information”, <https://www.facebook.com/help/203805466323736> (last accessed on 25 August 2015)

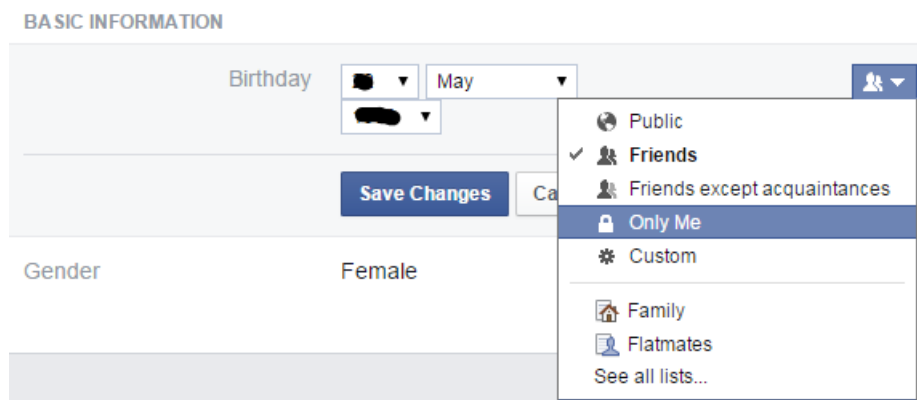
<sup>45</sup> Facebook, “When I post something, how do I choose who can see it?”, <https://www.facebook.com/help/120939471321735> (last accessed 25 August 2015).

## 2) Contact and Basic Info

Aside from the settings regulating access to “posts” (which is found under the Privacy Settings and Tools section), Facebook users can, to a certain extent, select their audience in relation to so-called “Contact and Basic Info”. This section can be found on the user’s profile page under the heading “About”<sup>46</sup> > “Contact and Basic Info”.

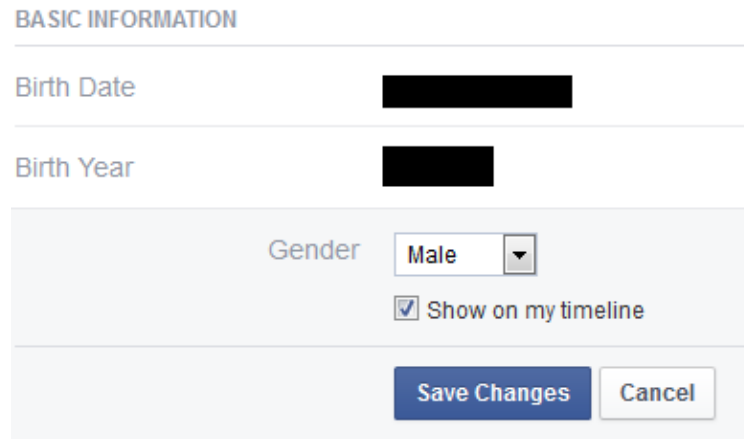


“**Basic Info**” first of all includes the users’ date of birth (day, month), their year of birth and their gender. This information is actively solicited by Facebook during registration and users are obliged to disclose this information to Facebook if they want to make use of the service. After the registration process has been completed, users can go back to the “Contact and Basic Info” section and select a specific audience for their date and year of birth. The default for date and year of birth is set to “Friends of friends”. Facebook offers separate settings for users’ “date of birth” and their “year of birth”, meaning that users can choose separately whether to share either their date and/or year (or nothing) with other Facebook users.



<sup>46</sup> The tab “About” is located in between the tabs “Timeline” and “Friends” on the Facebook user’s profile.

With regard to their gender, many users can only choose among “male” and “female”. If users choose between either “male” or “female”, they cannot choose a specific audience, but can only choose to show this information on their timeline or not (by ticking the box). By default, the box is ticked so the information is shown on their Timeline.<sup>47</sup>



BASIC INFORMATION

Birth Date [REDACTED]

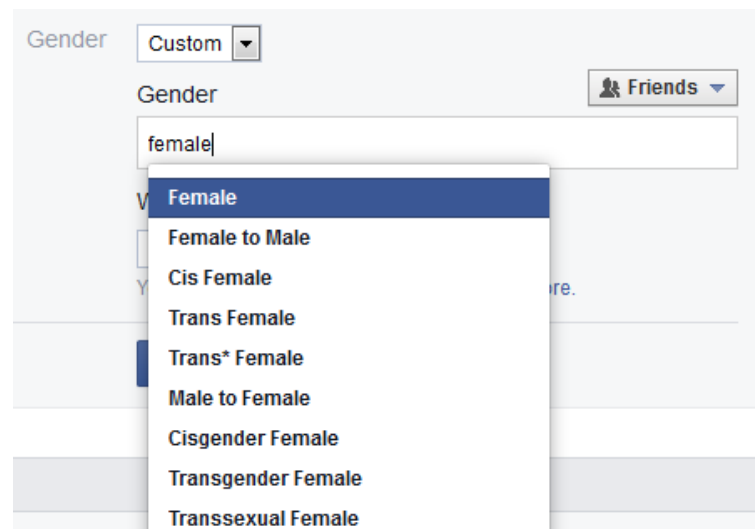
Birth Year [REDACTED]

Gender Male ▾

Show on my timeline

Save Changes Cancel

Since February 2015, certain users are also able to customise their gender settings by selecting “custom”<sup>48</sup>. At the moment, this setting appears to be available only for users who have selected “English US” as their Facebook language.



Gender Custom ▾

Gender Friends ▾

female|

- Female
- Female to Male
- Cis Female
- Trans Female
- Trans\* Female
- Male to Female
- Cisgender Female
- Transgender Female
- Transsexual Female

<sup>47</sup> Interestingly, “gender” is also listed under “Public Information” which according to Facebook is always publicly available (see also *infra* section 3.A.3).

<sup>48</sup> See also W. Oremus, “Facebook No Longer Limits Your Gender to “Male” or “Female”, *Slate Future Tense*, 13 February 2015, accessible at [http://www.slate.com/blogs/future\\_tense/2014/02/13/facebook\\_gender\\_options\\_male\\_female\\_and\\_custom\\_plus\\_preferred\\_pronouns.html](http://www.slate.com/blogs/future_tense/2014/02/13/facebook_gender_options_male_female_and_custom_plus_preferred_pronouns.html) (last accessed 25 August 2015).

Users who opt to “customise” their gender, are able to select its audience by choosing among “Friends”, “Public”, “Friends of friends”, “Only me” and “Custom”. Users are then asked to select their “preferred pronoun”, for which there is a wired-in “public” setting:

The screenshot shows a settings panel for gender and pronouns. At the top, there is a 'Gender' dropdown menu set to 'Custom'. Below it, a 'Gender' dropdown menu is set to 'Friends'. A text input field contains 'Trans Person' with a close button. The question 'What pronoun do you prefer?' is followed by a dropdown menu set to 'Neutral: "Wish them a happy birthday!"'. Below this, a message states 'Your preferred pronoun is Public. Learn more.' A blue information box contains the text 'Your preferred pronoun is Public and can be seen by anyone.' At the bottom, there are 'Save Changes' and 'Cancel' buttons.

Facebook users are also encouraged to share additional information (which Facebook also qualifies as “Basic Info”), including their sexual preference (“who you’re interested in”), the language(s) they speak, and their religious or political views. The default for sexual preference and language(s) is set to “Public”, but users can opt for the settings “Friends”, “Only me” and “Custom”. The default for religious or political views on the other hand is set to “Friends of friends” and users can select the following settings: “Public”, “Friends”, “Only Me” or “Custom”.

The screenshot shows the 'BASIC INFORMATION' section of a Facebook profile. It lists several fields: 'Birth Date' (blacked out), 'Birth Year' (blacked out), and 'Gender' (set to 'Male'). Below these fields are four blue links with plus signs: '+ Add who you're interested in', '+ Add a language', '+ Add your religious views', and '+ Add your political views'.

### 3) “Public Information” and “Public Profile”

Facebook labels certain information users share during registration as “**Public Information**”, which is said to be “always public”.<sup>49</sup> Public Information includes a user’s age range, language and country. In addition, Facebook also labels certain parts of users’ profiles as “**Public Profile**”, which is said to be “also public”. Public Profile includes a user’s name, gender, username and user ID, cover photo and networks such as school and workplace.<sup>50</sup>

#### What is public information?

Something that’s public can be seen by anyone. That includes people who aren’t your friends, people off of Facebook and people who use different media such as print, broadcast (ex: television) and other sites on the Internet. For example, if you use our services to provide a real-time public comment to a television show, that may appear on the show or elsewhere on Facebook.

#### What information is public?

**Information you share that is always public:** Some of the information you give us when you fill out your profile is public, such as your age range, language and country. We also use a part of your profile, called your Public Profile, to help connect you with friends and family. Your Public Profile includes your name, gender, username and user ID (account number), profile picture, cover photo and networks. This info is also public.

### 4) Search engines

In October 2013, Facebook eliminated the privacy setting “*Who can look up your Timeline by name*”.<sup>51</sup> The setting previously allowed users to control whether or not they would appear in any search engines “*on and outside of Facebook*”, when someone else typed in their first or last name in a search engine. Now, users can only choose whether they want to allow *other* search engines to link to their Timeline and can no longer exercise control over Facebook’s own internal search engine (i.e., the Facebook search bar).

Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	Yes	Edit

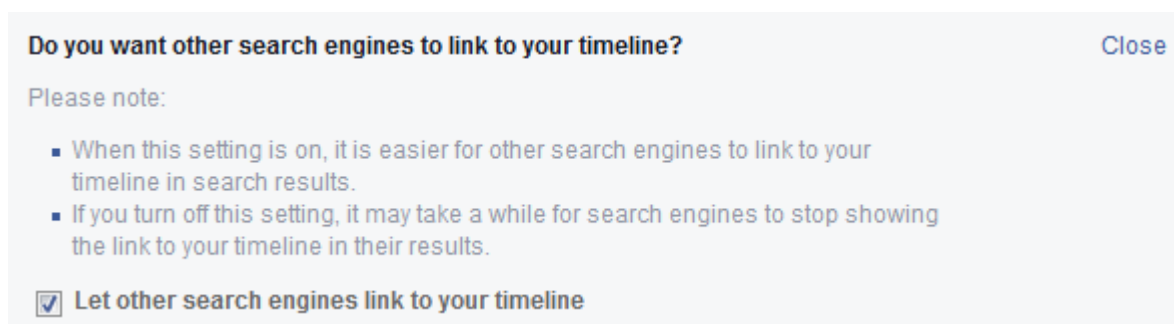
<sup>49</sup> Facebook, “What is public information?”, <https://www.facebook.com/help/203805466323736>, last accessed 25 August 2015.

<sup>50</sup> *Id.*

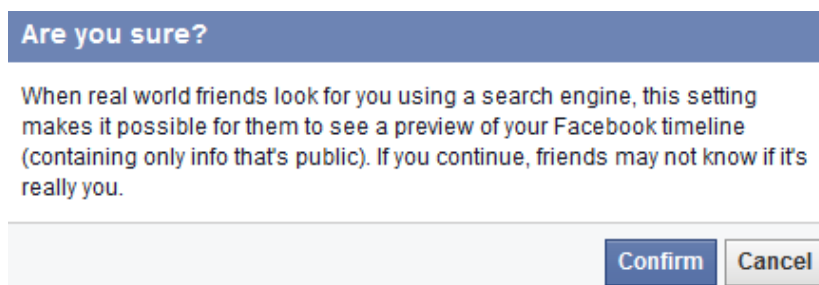
<sup>51</sup> For users who didn’t have the setting checked, it was already deleted the year before. See S.W. Lessin, “Better Controls for Managing Your Content”, 21 December 2012, <http://newsroom.fb.com/news/2012/12/better-controls-for-managing-your-content/>. See also <https://newsroom.fb.com/news/2013/10/reminder-finishing-the-removal-of-an-old-search-setting/>.



Users who decide to edit the search engine setting are asked whether they want “other” search engines to link to their Timelines.<sup>52</sup> Linking to their Timelines in fact means that information is shown which is publicly available.



The external search engine setting is turned on by default. If users want to turn off this setting, they get a message asking whether they are sure about their choice. When users choose to re-tick the box, no similar message appears (e.g., warning them that it will enable indexing of public Timeline information by external search engines like Google, Bing, etc.).



The removal of the previous setting effectively forced every user into Facebook’s “**Graph Search**”, which is an (internal) search feature operated by Facebook. With Graph Search, all data of other Facebook users which a user is able to see (but until then could only find with difficulty) has become searchable and more easily accessible.<sup>53</sup> Users can combine different search criteria (e.g., single men who like sewing) and can select different types of search results (i.e., People, Photos, Pages, Places, Groups, Apps and Events). Interesting to note is that the Graph Search function is only available for users who have selected “English US” as their Facebook language.<sup>54</sup>

---

<sup>52</sup> A Timeline is Timeline is the space on a user’s profile where users can see their own posts, posts from friends and stories in which they are tagged, organised by the date they were posted. (Facebook, “What is Timeline?”, accessible at <https://www.facebook.com/help/1462219934017791>, last accessed 25 August 2015).

<sup>53</sup> See also Maximillian Schrems, *Mag. Maximillian Schrems v. Facebook Ireland Limited*, Handelsgericht Wien, 31 July 2014, p. 28 et seq [http://www.europe-v-facebook.org/sk/sk\\_en.pdf](http://www.europe-v-facebook.org/sk/sk_en.pdf) (last accessed 24 August 2015).

<sup>54</sup> A. Verchère, “Facebook Graph Search : comment l’utiliser en marketing ?”, 30 September 2014, accessible at <http://siecledigital.fr/2014/09/facebook-graph-search-comment-lutliser-en-marketing>; Facebook, “Graph Search now Fully Launched in US English”, 7 August 2013, accessible at <https://newsroom.fb.com/news/2013/08/graph-search-now-fully-launched-in-us-english>.

The following examples illustrate how detailed and sensitive Graph Search can be, especially as there is no further context provided.<sup>55</sup>



See more

<sup>55</sup> As such "apparently harmless pieces of information, when assembled together, could reveal a damaging picture." (A. Melber, "Why Graph Search could be Facebooks largest privacy invasion ever, 12 January 2013, accessible at <http://www.thenation.com/article/why-graph-search-could-be-facebooks-largest-privacy-invasion-ever>, last accessed 24 August 2015).

Facebook users also have the ability to determine *who can “look them up”* by using either the email address or phone number they provided. The default setting for both settings is “Everyone”, which means that even individuals who do not have the permission to view an individual’s phone number may still be able to link his or her phone number with their Facebook Account.<sup>56</sup>

---

Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	<b>Who can look you up using the phone number you provided?</b>		Close
	This applies to people who can't already see your phone number.		
	<input type="button" value="Everyone"/>		
	Do you want other search engines to link to your Timeline?	No	Edit


---

## 5) “Friend list” and “Following”

Facebook users are given the opportunity to customise the audience of people who can see their list of friends as well as the people or pages they are following. This setting can be found on the user’s profile page, under the heading “Friends” (which is located next to the “About” heading).

### Who can see the Friends section of my profile?

By default, everyone can see the **Friends** section of your profile. To adjust who can see your **Friends** section:

1. Go to your profile
2. Click **Friends** below your cover photo
3. Click  at the top of the page and select **Edit Privacy** from the dropdown menu
4. Select an audience (ex: **Friends**, **Public**) to choose who you share your friend list with on your profile

Users can select their audience when it comes to their Friend list, under the heading “Friends” on their profile. The default is set to “Public”, but users can opt for the settings “Friends”, “Only me” and “Custom”.<sup>57</sup>

---

<sup>56</sup> In August 2015, a software developer was able to harvest data about thousands of users by guessing their mobile numbers. See J. Halliday, “Facebook urged to tighten privacy settings after harvest of user data”, The Guardian, 10 August 2015, accessible at <http://www.theguardian.com/technology/2015/aug/09/facebook-privacy-settings-users-mobile-phone-number> (last accessed 10 August 2015).

<sup>57</sup> See also Facebook, “Who can see the Friends section of my profile?”, accessible at [https://www.facebook.com/help/115450405225661/?ref=timeline\\_about](https://www.facebook.com/help/115450405225661/?ref=timeline_about) (last accessed 24 August 2015). It

### Edit Privacy ✕

---

**Friend List**

Who can see your friend list? Public ▾

Remember: Your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in news feed, search and other places on Facebook. They'll also be able to see mutual friends on your timeline.

---

**Following**

Who can see the people and lists you follow? Public ▾

Remember: The people you follow can see that you're following them.

---

[Learn More](#)
Done

## 6) “Timeline” and “Tagging”

Every Facebook user profile has an associated “**Timeline**”, described as

*“the space on your profile where you can see your own posts, posts from friends and stories you're tagged in organized by the date they were posted”.*<sup>58</sup>

Facebook offers its users the ability to determine whether **posts made by others** will appear on their Timeline. The default setting is to allow all “Friends” to post to one’s Timeline:

- ⚙️ General
- 🔒 Security

---

- 🔒 Privacy
- 📅 **Timeline and Tagging**
- 🚫 Blocking

---

- 📧 Notifications
- 📱 Mobile
- 📊 Followers

---

- 📱 Apps
- 📄 Ads
- 💳 Payments
- 📧 Support Inbox
- 📺 Videos

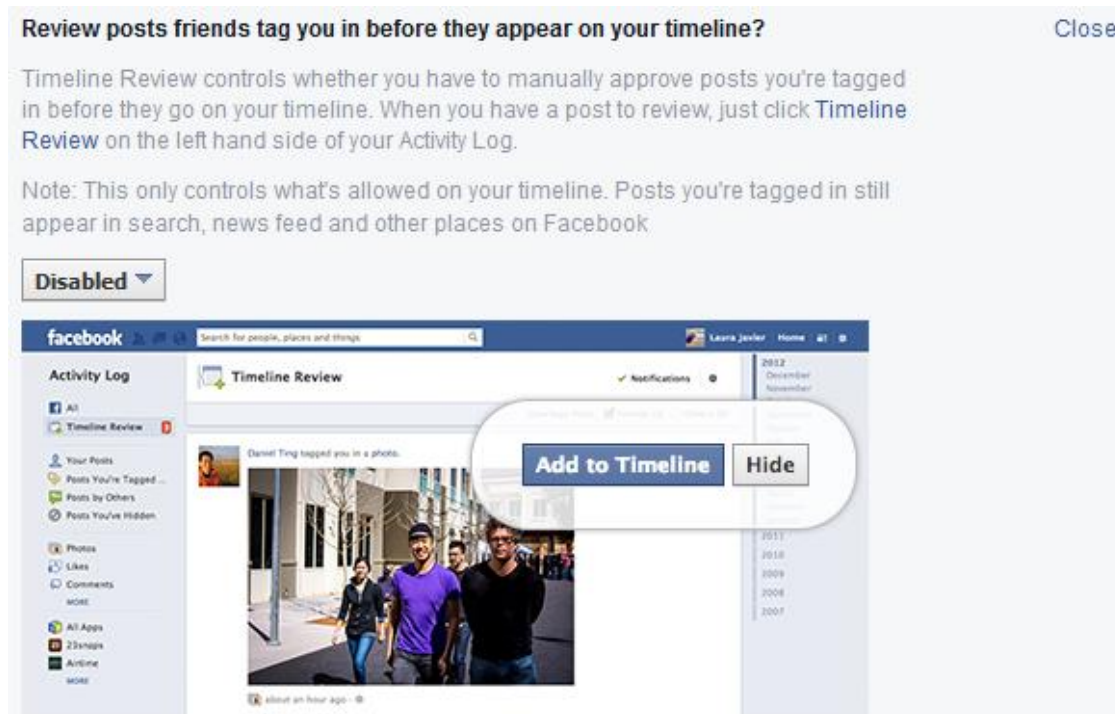
### Timeline and Tagging Settings

<b>Who can add things to my timeline?</b>	Who can post on your timeline?	Friends	<a href="#">Edit</a>
	Review posts friends tag you in before they appear on your timeline?	Off	<a href="#">Edit</a>
<b>Who can see things on my timeline?</b>	Review what other people see on your timeline		<a href="#">View As</a>
	Who can see posts you've been tagged in on your timeline?	Friends of Friends	<a href="#">Edit</a>
	Who can see what others post on your timeline?	Friends	<a href="#">Edit</a>
<b>How can I manage tags people add and tagging suggestions?</b>	Review tags people add to your own posts before the tags appear on Facebook?	Off	<a href="#">Edit</a>
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	<a href="#">Edit</a>
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

should be noted, however, that even if users restrict the accessibility of their Friends list (e.g. to “Friends only” or “Only me”), this may not prevent applications from obtaining this permission: cf. *infra* section 3.B.

<sup>58</sup> Facebook, “What is Timeline?”, accessible at <https://www.facebook.com/help/1462219934017791>, last accessed 24 August 2015.

Users may also activate “*Timeline Review*”, which enables them to manually approve every post in which they are tagged before it appears on their Timeline. The default setting for Timeline Review is “Off”. Activating Timeline Review does not restrict the visibility of the posts in search, news feed or other places on Facebook:



Facebook users can also manage “the tags people add” in a separate setting, which is referred to as “Tag Review”. “**Tagging**” is described by Facebook as follows:

*“When you tag someone, you create a link to their profile. The post you tag the person in may also be added to that person’s [Timeline](#). For example, you can tag a photo to show who’s in the photo or post a status update and say who you’re with. If you tag a friend in your status update, anyone who sees that update can click on your friend’s name and go to their profile. Your status update may also show up on that friend’s Timeline.*

*When you tag someone, they’ll be notified. Also, if you or a friend tags someone in your post, the post could be visible to the audience you selected plus friends of the tagged person. Learn more about what happens when you [create a tag](#).*

*Tags in photos and posts from people you aren’t friends with may appear in [Timeline review](#) where you can decide if you want to allow them on your Timeline. You can also choose to review tags by anyone, including your friends.”<sup>59</sup>*

<sup>59</sup> Facebook, “What is tagging and how does it work?”, accessible at <https://www.facebook.com/help/124970597582337> (last accessed 25 August 2015).

Tag review is disabled by default, which means that any “Friend” will be able to add tags to a user’s post by default. Tags added by someone who is not a “Friend” are subject to prior approval by default:

How can I manage tags people add and tagging suggestions?

Review tags people add to your own posts before the tags appear on Facebook?

Close

Turn on Tag Review to review tags friends add to your content before they appear on Facebook. When someone who you're not friends with adds a tag to one of your posts you'll always be asked to review it.

Remember: When you approve a tag, the person tagged and their friends may be able to see your post.

Disabled ▾



When you're tagged in a post, who do you want to add to the audience if they aren't already in it?

Friends

Edit

Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)

Unavailable

It is important to note that the Tag Review feature **only extends to** tags which are added to the “**own posts**” of a user, meaning that other instances in which a user is tagged (e.g., in someone else’s Timeline) cannot be prevented by the user in advance. Outside of their own posts, users can only (a) “untag” themselves after the fact; (b) limit the visibility of such posts on their own Timeline; or (c) block the user who is tagging them against their will.

## B. Application settings

With regard to Facebook’s application settings, a distinction should be made between (1) applications which users have downloaded themselves and (2) applications downloaded by their friends.

### 1) Applications which users download themselves

In the introductory text under the heading “App Settings”, Facebook states that

*“On Facebook, your name, profile picture, cover photo, gender, networks, username, and user ID are always publicly available to both people and apps. [Learn why](#). Apps also have access to your Friends list and any information you choose to make public”<sup>60</sup>*

In other words, Facebook states that the following categories information are **always accessible** to application providers:

- (1) a user’s name;
- (2) profile picture;
- (3) cover photo;
- (4) gender;
- (5) networks;
- (6) username; and
- (7) user ID
- (8) friends list<sup>61</sup>; and
- (9) any information users decide to make public.

It is worth noting that Facebook employs **different definitions** of certain categories of information in the apps context in comparison to the social privacy context. For instance, “**Public Profile**” is defined more broadly in the apps context, as it includes the user’s age range, language and country (which is elsewhere labelled as “Public Info”). A more striking example is the category “**Basic Info**”, which seems to refer to entirely different pieces of information in the two contexts. The following table provides an overview of the different definitions regarding certain

---

<sup>60</sup> Facebook, “App settings”, accessible at <https://www.facebook.com/settings?tab=applications>, last accessed 25 August 2015.

<sup>61</sup> In April 2015, Facebook issued the following statement “A year ago, we announced that apps would no longer receive a person’s entire friend list, only the friends who already use the app and only if people choose to share this list. That policy is already in effect for many apps, and it goes into effect for all apps on April 30, 2015.” See R. Allen, “Setting the record straight on a Belgian academic report”, 8 April 2015, <http://newsroom.fb.com/news/h/setting-the-record-straight-on-a-belgian-academic-report/>. To date, the user interface stating that all applications have access to a user’s Friends List has not been updated. Facebook’s Data Use Policy also still indicates that “when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them.” (last verified 25 August 2015).

categories of information and allows a comparison between the social privacy context and the apps context:

	Basic Info	Public Profile	Public Information
<i>Social privacy context</i>	<p>According to Home &gt; about &gt; settings:</p> <ul style="list-style-type: none"> <li>• date of birth</li> <li>• year of birth</li> <li>• gender</li> <li>• sexual preference</li> <li>• language</li> <li>• religious views</li> <li>• political views</li> </ul>	<p>According to the Help page hyperlinked in the 2015 DUP <sup>62</sup></p> <ul style="list-style-type: none"> <li>• name</li> <li>• gender</li> <li>• user name</li> <li>• user ID</li> <li>• profile picture</li> <li>• cover photo</li> <li>• networks</li> </ul>	<p>According to the Help page hyperlinked in the 2015 DUP <sup>63</sup></p> <ul style="list-style-type: none"> <li>• public profile <ul style="list-style-type: none"> <li>○ name</li> <li>○ gender</li> <li>○ username</li> <li>○ userID</li> <li>○ profile picture</li> <li>○ cover photo</li> <li>○ networks</li> </ul> </li> <li>• age range</li> <li>• language</li> <li>• country</li> <li>• information shared publicly (e.g., public posts, profile information set to public)</li> </ul>
<i>Apps context</i>	<p>According to user interface for “Instagram”:</p> <ul style="list-style-type: none"> <li>• name</li> <li>• userID</li> <li>• profile picture</li> <li>• gender</li> <li>• list of friends</li> <li>• any other information you made public (not defined)</li> </ul>	<p>According to the user interface for “Juice Jam”:</p> <ul style="list-style-type: none"> <li>• name</li> <li>• gender</li> <li>• profile picture</li> <li>• age range</li> <li>• language</li> <li>• country</li> <li>• other public info (not defined).<sup>64</sup></li> </ul>	Not defined.

<sup>62</sup> Facebook, “What is public information?”, accessible at <https://www.facebook.com/help/203805466323736> last accessed 25 August 2015.

<sup>63</sup> *Id.*

<sup>64</sup> The overview of “Public Profile” information shown in the user interface is notably shorter than the list which Facebook maintains on a separate Help page. Compare Facebook, “What info do apps receive when they access my public profile”, accessible at <https://www.facebook.com/help/145506622264765> (last accessed 25 August 2015). The separate Help Page states that application providers will access: (1) name; (2) gender; (3) username; (4) userID; (5) profile picture; (6) network; (7) age range; (8) language; (9) country and (10) other info you choose to make public. According to yet another (app-specific) Help page, applications also have access to other information, including Friends lists. See Facebook, “Why is an app requesting to access my info?”, accessible at <https://www.facebook.com/help/187333441316612> (last accessed 25 August 2015). (“Keep in mind when you install an app, you give it permission to access your **public profile**, which includes your name, profile pictures, username, user ID (account number), networks and any info you choose to make publicly available. **You also give the app other info** to personalize your experience, including your friends list, gender, age range and locale.”)



**Juice Jam**  
SGN

It's Jam Time!

Match. Juice. Serve. Repeat! The creators of hit game, Cookie Jam, present a juicy new matching puzzle game with bushels of fruity challenges! Hop in the j... Read more

46,501 likes  
1 million players

Addictive Challenging Match 3

**Play Now**

Your public profile includes name, profile picture, age range, gender, language, country and other public info

By clicking on "Play Now" above, Juice Jam will receive the following info: your public profile.

Review the info you provide

By proceeding, you agree to Juice Jam's Privacy policy.

Block  
Report a Problem

**Instagram**  
Instagram, Inc.

Capture and share the world's mom...

It's a simple way to capture and share the world's moments on your iPhone. Customize your photos and videos with one of several gorgeous and custom built... Read more

28,136,215 likes  
150 million users

**Send to Mobile**

This app may post on your behalf, including objects you commented on, objects you liked and more.

By clicking "Send to Mobile" above, Instagram will receive: Includes your name, Profile picture, gender, user ID, list of friends and any other information you made public

Your basic info [?]

Friends

By proceeding, you agree to Instagram's Terms of Service and Privacy policy.

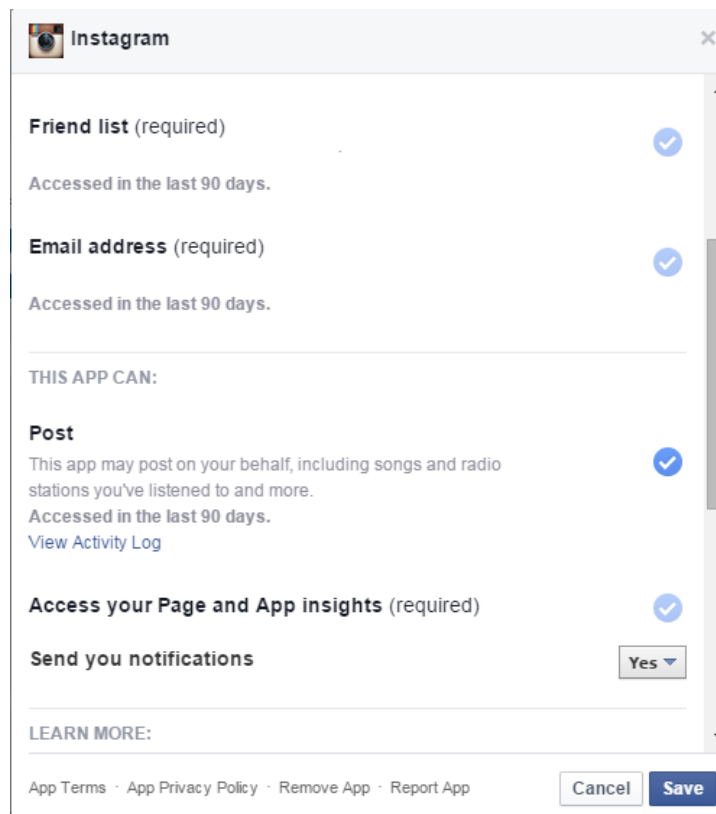
Report a Problem

## ***Default vs. wired-in settings***

Users can, to a certain extent, edit the information they share with apps before beginning to use a specific app (on an opt-out basis). Specifically, limited options are available to restrict

- (1) app visibility towards other users;
- (2) data collection by app providers (but actual controls vary from app to app); and
- (3) posting on behalf of the user.

For example, the following screenshot shows the application settings for Instagram:



Users are able to change the full blue settings, simply by clicking on them. The greyed-out settings are wired-in, which means that users cannot change them. For Instagram, users can choose whether the app can post on their behalf. On the other hand, users do not have control over Instagram's access to their email address or Friend list.<sup>65</sup> As mentioned, these settings may vary from app to app. For instance, for the app iPhoto, users can choose whether or not to share photos and videos, or their friends' chat statuses. However, users cannot control that iPhoto posts on their behalf, as this setting is wired-in.

---

<sup>65</sup> It is important to note that there are others applications where Friends List is pre-checked by default but users do have an option to opt out. So the default as well as the wired-in settings may vary from app to app.

## 2) Applications downloaded by friends

Facebook users can, to a certain extent, enable application providers to **access their friends' data**.<sup>66</sup> Facebook indicates as much under its App settings, under the title “*Apps Others Use*”. Users are offered settings to control the categories of information their friends can bring with them when using apps. By default, many types of information can be made accessible to application providers, as most boxes are pre-checked:

### Apps others use ×

People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

<input checked="" type="checkbox"/> Bio	<input checked="" type="checkbox"/> My videos
<input checked="" type="checkbox"/> Birthday	<input checked="" type="checkbox"/> My links
<input checked="" type="checkbox"/> Family and relationships	<input checked="" type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input checked="" type="checkbox"/> Home Town
<input type="checkbox"/> Religious and political views	<input checked="" type="checkbox"/> Current location
<input checked="" type="checkbox"/> My website	<input checked="" type="checkbox"/> Education and work
<input checked="" type="checkbox"/> If I'm online	<input checked="" type="checkbox"/> Activities, interests, things I like
<input checked="" type="checkbox"/> My status updates	<input checked="" type="checkbox"/> My app activity
<input checked="" type="checkbox"/> My photos	

If you don't want apps and websites to access other [categories of information](#) (like your friend list, gender or info you've made public), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.

In addition, the text shown above indicates that apps and websites may be able to access other categories of information, like users' friend lists, their gender or information they've made public.<sup>67</sup> The only way for users to prevent this is to turn off the application platform entirely (which would mean that his or her information cannot be accessed by any application). Turning off the platform would also imply, however, that users no longer can make use of certain features on external websites (see next section).<sup>68</sup>

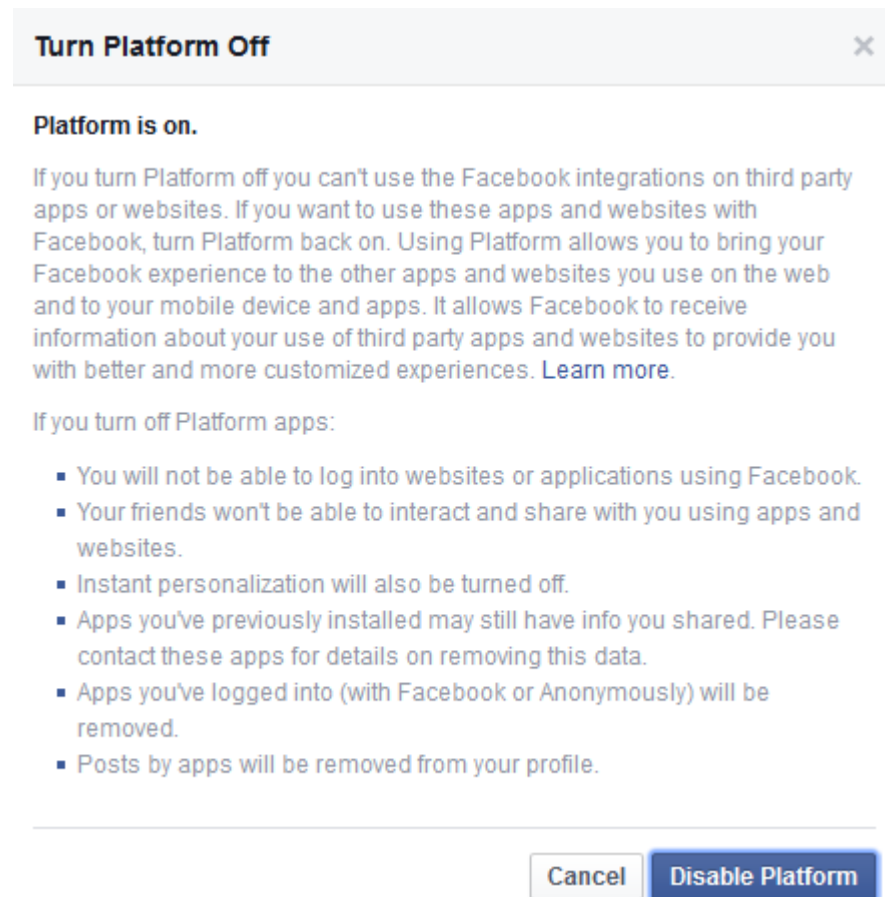
<sup>66</sup> See also A. Helmond, “The new Facebook data policy: like or dislike?”, *Internet Policy Review*, 2 December 2014, accessible at <http://policyreview.info/articles/news/new-facebook-data-policy-or-dislike/341>.

<sup>67</sup> Application providers must specifically request users for permission to access their Friends' information, except for “basic information”. The “basic information” will be accessible to application providers by default, regardless of permissions. See D. O'Reilly, ‘Report on Facebook Ireland (FB-I) Audit 2-3 May & 10-13 July 2012’, 21 September 2012, p. 20, [https://dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf), (last accessed 3 August 2015). Regarding the default accessibility of a user's Friends List see also *supra*; section 3.B.1.

<sup>68</sup> The Irish DPC in its 2012 Re-Audit also recommended Facebook to provide a more granular choice and control to its users in this area. See Irish Data Protection Commissioner, *Facebook Ireland Ltd – Report of Re-Audit*, 21 September 2012, 31,

### 3) Platform setting

Under the heading “*Apps, websites and plug-ins*”, users are provided the ability to “Disable Platform”. Doing so will prevent third-party applications from accessing their personal data (including applications downloaded by Friends). It also entails, however, that users can no longer make use of applications themselves or make use of any Facebook integrations on third party websites, such as “Facebook Login” or “Like” buttons:



If a user decides to “Disable the Platform” and later seeks to re-enable it, it will “reset related settings” (such as your “Apps others use” setting) and allow Facebook to once again receive information about his or her use of third party apps and websites.

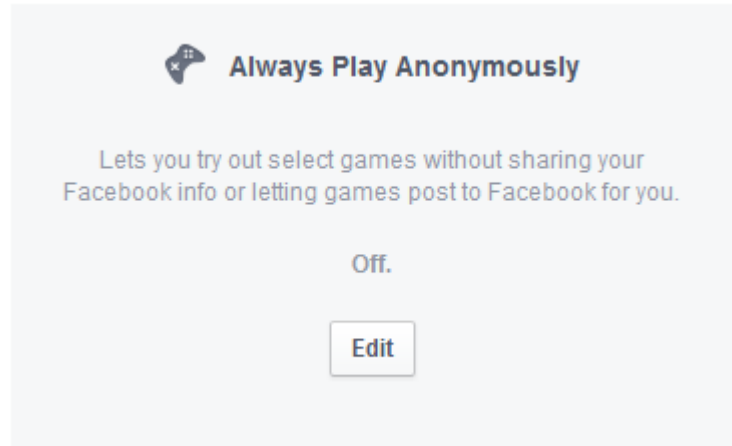
---

[https://www.dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf)

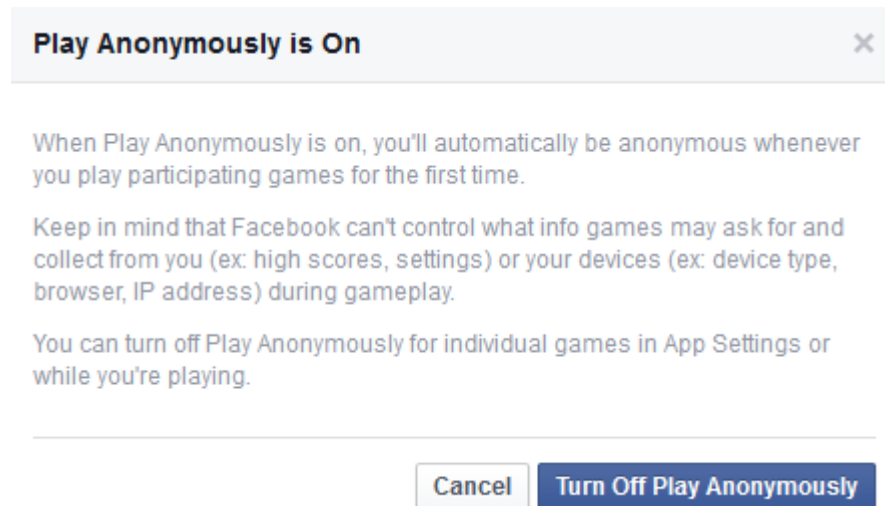
(“However it should be made easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way at present to manage this is to turn off all apps via a user’s privacy settings but this also prevents the user from using apps themselves.”) Already in 2009, the Canadian DPC recommended Facebook to prohibit application providers to accessing personal information of users who are not themselves adding an application. See E. Denham, “Report of the findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.”, 16 July 2009, 54 (para 211).

#### 4) Play anonymously

Under the App Settings, Facebook users also have an option to “Always Play Anonymously”:



When activated (by default the setting is turned off), the setting should allow users to login to select games without having to share any personal information or permissions<sup>69</sup>



The “Play Anonymously” function is **only available for a limited number of apps**. In addition, if users choose (or have chosen) to use Facebook Login for a certain app, they cannot switch to Anonymous Login later (whereas the other way around is possible).<sup>70</sup>

<sup>69</sup> See also Facebook, “How does Anonymous Login differ from Facebook Login?”, accessible at <https://www.facebook.com/help/536380663149455> (last accessed 25 August 2015) (“However, while Facebook Login gives you the option to share your personal info with the app or game, Anonymous Login shares none of your info. It also doesn't allow the app or game to post on your behalf.”).

<sup>70</sup> Facebook, “If I use Anonymous Login, can I later choose to use Facebook Login?”, accessible at <https://www.facebook.com/help/1423106354612316> (last accessed 25 August 2015).

## C. Advertising settings

Facebook's settings for advertising can be found under the heading "Facebook Ads", which is an additional setting, separate from the privacy settings. The settings currently offered for advertising are essentially two-fold: (1) a setting for "Ads and Friends" and (2) a setting for "Ads Based On Your Use Of Websites Or Apps Off Facebook".<sup>71</sup>

### 1) Ads and Friends

Under the heading "Ads and Friends", users are given the opportunity to opt out from appearing in so-called "Social Ads". A Social Ad is an advertisement which links promotional content with actions performed by Facebook users (e.g., liking a page) and their name and/or profile picture.<sup>72</sup> Users can opt out from appearing in Social Ads, but cannot opt out from appearing in so-called "Sponsored Stories"<sup>73</sup>:

**Adverts and Friends**


Everyone wants to know what their friends like. That's why we pair adverts and friends — an easy way to find products and services you're interested in, based on what your friends share and like. [Learn more about social adverts.](#)

Here are the facts:

- Social adverts show an advertiser's message alongside actions you have taken, such as liking a Page
- Your privacy settings apply to social adverts
- We don't sell your information to advertisers
- Only confirmed friends can see your actions alongside an advert
- If a photo is used, it is your profile photo and not from your photo albums


**Here's an example of a Facebook advert:**

**Denver sushi**



The best sushi in Denver. Try our daily lunchtime specials for \$9.95. Become a fan of our page for special offers.

**Denver sushi**



The best sushi in Denver. Try our daily lunchtime specials for \$9.95. Become a fan of our page for special offers.

Like · Louisa Peeters likes Denver sushi.

This setting only applies to adverts that we pair with news about social actions. So regardless of this setting, you may still see social actions in other contexts, like in sponsored stories or paired with messages from Facebook. You can learn more about how social adverts, sponsored stories and messages from Facebook work in the [Help Centre](#).

Pair my social actions with adverts for

[Save Changes](#) [Cancel](#)

<sup>71</sup> Facebook's Ads settings also include a setting for "Third Party Sites", where it states that "Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used." As this setting is not yet relevant we do not analyse it further for the time being.

<sup>72</sup> See also Facebook, "About advertising on Facebook", accessible at <https://www.facebook.com/about/ads> and Facebook, "When will my ad show with social information?" accessible at <https://www.facebook.com/help/1447178318880237> (last accessed 25 August 2015).

<sup>73</sup> A Social Ad is not the same as a Sponsored story. Sponsored stories appear in users' News Feed while social ads appear in a box on the right hand side, designated for advertising. See also *infra*; Section 7.B.

## 2) Behavioural advertising

By default, Facebook will collect and use information regarding users' activities off of Facebook for ad targeting purposes. Under the heading "Ads Based on Your Use of Websites or Apps Off Facebook", users are informed that they can opt out of tracking and targeted advertising by providing **links to the websites** of the American, Canadian and **European Digital Advertising Alliance**.<sup>74</sup>

### Ads Based On Your Use Of Websites Or Apps Off Facebook

#### Ads Based On Your Use Of Websites Or Apps Off Facebook

One of the ways ads reach you is when a business or organization asks Facebook to show their ads to people who have used their websites and apps off Facebook. For example, you might visit a company's website that uses cookies to record visitors to it. The company then asks Facebook to show their ad to this list of visitors, and you might see these ads both on and off Facebook. This is a type of interest-based advertising.

If you don't want Facebook or other participating companies to collect or use information based on your activity on websites, devices, or apps off Facebook for the purpose of showing you ads, you can opt out through the **Digital Advertising Alliance** in the USA, **Digital Advertising Alliance of Canada** in Canada or the **European Digital Advertising Alliance** in Europe. You can also opt out using your mobile device settings.

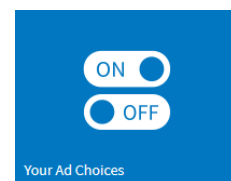
You only need to opt out once. If you opt out of interest-based advertising from Facebook on one phone or computer, we'll apply that choice everywhere you use Facebook.

Once arrived at the website of the European Digital Advertising Alliance (<http://www.youronlinechoices.eu>), the user will be asked to select his or her location. The user must then navigate to "Your Ad Choices", at which point the site collects the users' "status" from the participating companies. Once complete, the individuals can either "turn off" individual companies one by one or scroll down to the setting "turn off all companies".



## Your Online Choices

a guide to online behavioural advertising



### Your ad choices

The companies listed below are some of the providers who work with website providers to collect and use information to provide online behavioural advertising.

Please use the buttons below to control your online behavioural advertising preferences. You can turn off or turn on all companies or alternatively set your preferences for individual ones. By clicking on the expand button you can find out more about the company itself as well as its behavioural advertising status on the web browser that you are using. If you are having any problems please visit our [help page](#).

Please note: this does not turn off all internet advertising, only advertisements that are collecting your status from 102 companies. This may take a while...

**Some Companies Failed:** The tool was unable to connect to some companies. This may be because there are technical problems with the service or your internet connection is very busy. We have automatically logged this failure and will contact the company if the problem persists.



<sup>74</sup> See also *infra*; Chapter 8 Tracking through social plug-ins.

## D. Assessment

Adjustable privacy settings can serve as an additional way to obtain consent for certain specific types of data processing. Because of their adjustability, settings can be understood as the expression of the user's will. According to the Article 29 Working Party, however, the provider of an online social network should offer default settings<sup>75</sup>

*"which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties".<sup>76</sup>*

In other words: **access to profile information should be restricted to self-selected contacts** (i.e., "Friends") **by default**. Users should be asked for permission before access is extended to any other entity.<sup>77</sup> Facebook does not restrict access to profile information to self-selected contacts by default. Moreover, certain key settings are missing, thereby limiting the control Facebook users can exercise in relation to the processing of their personal data.

### 1) False sense of control

Facebook's privacy settings offer users considerable control when it comes to regulating access of their data by other users ("social privacy"). Control is considerably less granular in relation to the collection and/or use of data by Facebook itself or by third-parties. This gives users a false sense of control. Moreover, the language used in the *Privacy Basics* tutorial, employs phrases such as "you're in charge" or "take control over who sees what you share on Facebook", which may actually mislead certain users (especially as the tutorial will not walk users through advertising or application settings).<sup>78</sup> In this regard, it is also worth noting that Facebook has chosen not to comply with the Irish DPC's recommendation to move the setting on Social Ads to the privacy settings section, in order to improve its accessibility.<sup>79</sup>

---

<sup>75</sup> In this regard, the Article 29 Working Party has advocated robust security and privacy-friendly default settings as "the ideal starting point with regard to all services on offer". (See Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 3, [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf)). Furthermore, concept of privacy by default has also been introduced in the article 23 of the proposed General Data Protection Regulation.

<sup>76</sup> Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 7.

<sup>77</sup> This includes access to personal data by application providers, including when this application has not been downloaded by the OSN user herself, but rather by one of her contacts.

<sup>78</sup> In this regard, it is worth mentioning that the US Federal Trade Commission in its Facebook consent order of 2011 ordered that Facebook: "shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of [...] its collection or disclosure of any covered information". FTC, *Agreement containing consent order in the matter of Facebook inc*, 2011, p. 4, accessible at <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>

<sup>79</sup> See Irish Data Protection Commissioner, *Facebook Ireland Ltd – Report of Re-Audit*, 21 September 2012, 18, [https://www.dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf).



## 2) Inconsistent definitions

Facebook employs different definitions for certain categories of information (i.e. “Basic Info”, “Public Profile” and “Public Information”) in different contexts. Users may thus easily be confused about which categories of data are available to whom, as the definitions sometimes vary. Facebook should ensure that terms are used consistently across the Data Use Policy, user interfaces and Help pages. In addition, Facebook does not clearly identify all the information requested by application providers at the moment they are being requested. Specifically, it will not always be very clear to users what “other public info” refers to when accessing an application, if it is not explicitly defined at the moment when the user is being asked to grant permission.

## 3) Insufficient control over indexation

According to the Article 29 Working Party, information contained in a user’s profile should not be made available for indexation by (internal or external) search engines unless the user has unambiguously agreed to this.<sup>80</sup> While Facebook states<sup>81</sup> that Facebook search respects users’ privacy settings, the potential for heightened interference with an individual’s privacy implies that individuals should have the ability to choose freely and specifically whether or not to be indexed by Facebook’s internal search engine.<sup>82</sup>

## 4) Insufficient tag controls

Facebook’s Tag Review feature only extends to tags which are added to a user’s “own posts”, meaning that other instances in which a user is tagged (e.g., on someone else’s Timeline, in a comment) cannot be prevented by the user in advance. Outside of their own posts, users can only (a) “untag” themselves after the fact; (b) limit the visibility of such posts on their own Timeline; or (c) block the user who is tagging them against their will.

In its 2011 Report of Audit, the Irish DPC observed that “[t]here does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it.”<sup>83</sup> In its 2012 Report of Re-Audit, the Irish DPC reconsidered its earlier position, and stated that “[t]aking account of the various tools available to users to manage tags and delete them if they so wish we

---

<sup>80</sup> See Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking’, l.c., p. 7 (“Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location”).

<sup>81</sup> Facebook, “Search privacy”, accessible at <https://www.facebook.com/help/www/468080906543413> (last accessed 26 July 2015) (“Facebook search respects privacy settings, which means people can search for info about you that they can see on Facebook, based on what’s been shared with them.”).

<sup>82</sup> See also Maximillian Schrems, *Mag. Maximillian Schrems v. Facebook Ireland Limited*, Handelsgericht Wien, 31 July 2014, p. 28 et seq [http://www.europe-v-facebook.org/sk/sk\\_en.pdf](http://www.europe-v-facebook.org/sk/sk_en.pdf) (last accessed 24 August 2015) (arguing that users’ prior opt-in consent should be obtained). See also E. Denham, “Report of the findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.”, 16 July 2009, 25 (para 94), accessible at [https://www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.pdf](https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf).

<sup>83</sup> Data Protection Commissioner, ‘Facebook Ireland Ltd. - Report of Audit’, 21 December 2011, p. 128, available at <http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf>.

are not requiring an ability to prevent Tagging at this time”.<sup>84</sup> In response, *Europe v. Facebook* argued that:

*“The fact that there is now a “review” function, which controls the visibility of tags, is a factual improvement but irrelevant under the law as the DPA does apply to “invisible” data just like it applies to visible data. There is still no consent for the use such “invisible” data that is processed by FB-I.”*<sup>85</sup>

While the ability to review and remove tags are valuable features, there still does not appear to be a compelling case as to why Facebook users should not be able to prevent tagging altogether or to subject all tags to prior approval. Moreover, certain language used by Facebook could be misconstrued by users to mean that enabling Tag Review will allow them to review tags for *all* content before it appears *anywhere* on Facebook.<sup>86</sup> However, the Tag Review feature only extends to tags which are added to the “own posts” of a user, meaning that other instances in which a user is tagged (e.g., in someone else’s Timeline) will not be subject to prior review.

## **5) Apps downloaded by friends**

Facebook users can authorise application providers to access certain data about their friends. In addition, application providers will have access to certain “basic information” by default.<sup>87</sup> Already in 2009, the Canadian DPC called upon Facebook to “*to prohibit all disclosures of personal information of users who are not themselves adding an application*”.<sup>88</sup> The current default settings for “Apps others use”, however, still entail that many types of information will be shared with third-party applications even if the individual concerned has not added the application.

While Facebook users can “turn off” the application platform entirely, such an option is unattractive as it will prevent them from accessing apps themselves. In its 2012 Re-Audit, the Irish DPC recommended Facebook to provide “more granular choice and control” in this area<sup>89</sup>:

*“[I]t should be made easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way at present to manage this is to turn off all apps via a user’s privacy settings but this also prevents users from accessing applications themselves.*

---

<sup>84</sup> See Irish Data Protection Commissioner, *Facebook Ireland Ltd – Report of Re-Audit*, 21 September 2012, p. 48, [https://www.dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf).

These controls are: 1) notice of tags; 2) the ability to pre-approve tags before appearing on one’s timeline; 3) the ability to un-tag; and 4) the ability to review tags other’s add to one’s own posts and 5) blocking (*Ibid*, p. 47).

<sup>85</sup> *Europe v. Facebook*, “Involuntary response to FB-I’s submissions”, *Europe v. Facebook.org*, 31 October 2013, accessible at [http://www.europe-v-facebook.org/Response\\_pub.pdf](http://www.europe-v-facebook.org/Response_pub.pdf) (last accessed 29 July 2015). *Europe v. Facebook* goes on to indicate that is in fact not possible for users to fully delete tags (*Id.*)

<sup>86</sup> “Turn on Tag Review to review tags friends add to your content before they appear on Facebook.”

<sup>87</sup> Cf. *supra*; section 3.B.2.

<sup>88</sup> E. Denham, “Report of the findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.”, 16 July 2009, p. 54 (paragraph 211).

<sup>89</sup> See Irish Data Protection Commissioner, *Facebook Ireland Ltd – Report of Re-Audit*, 21 September 2012, 31, [https://www.dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf).

*This Office had anticipated that FB-I would examine introducing means for a user who did not wish for anything other than basic data to be available to apps installed by their friends without having to actually take the drastic step of turning off Apps altogether.”<sup>90</sup>*

Facebook’s default configuration for “Apps Others Use” results in the disclosure of information about users which they have not unambiguously consented to. Instead of being required to opt out, Facebook users should be asked to authorise the disclosure of their personal data before such disclosures take place.<sup>91</sup> The current practice does not meet the requirements for legally valid consent.

## 6) Complex opt-out mechanisms

Facebook places considerable burden on users that wish to limit the disclosure of their personal data to self-selected contacts. Users are expected to navigate Facebook’s complex web of settings (which include “Privacy”, “Apps”, “Ads”, “Followers”, etc.) in search of possible opt-outs.

Users who do not want information about their activities on “websites, devices or apps off Facebook” to be used for advertising purposes, are faced with a particularly complicated and cumbersome opt-out mechanism. European users that wish to opt out must (1) navigate to “more settings”, (2) select “Adverts”, (3) click on the hyperlink of the European Digital Advertising Alliance, (4) select their location, (5) navigate to their ad choices, (6) select the companies one by one or scroll down to the setting “turn off all companies”.

The Article 29 Working Party has clarified that an opt-out mechanism “*is not an adequate mechanism to obtain average users informed consent*” for purposes of online behavioural advertising.<sup>92</sup> As a result, Facebook’s opt-out approach for online behavioural advertising **does not meet the requirements for legally valid consent**.<sup>93</sup> Moreover, it is important to note that **certain key settings are missing**, which means users cannot exercise control over these activities. For example, Facebook does not provide users with an opportunity to opt out of appearing in Sponsored Stories<sup>94</sup> or the sharing of location data<sup>95</sup> with Facebook.

Other problematic default settings include: (1) sexual preference (public by default); (2) look-up via email or phone number (authorised by default); (2) linking to external search engines (authorised by default); (3) friends list and following (public by default); and (4) the information which will by default be made accessible to application providers when adding the application (sometimes “wired-in”).

---

<sup>90</sup> *Id.*

<sup>91</sup> Europe v. Facebook, “Involuntary response to FB-I’s submissions”, Europe v. Facebook.org, 31 October 2013, p. 25-26, accessible at [http://www.europe-v-facebook.org/Response\\_pub.pdf](http://www.europe-v-facebook.org/Response_pub.pdf) (last accessed 29 July 2015). See Maximillian Schrems, *Mag. Maximillian Schrems v. Facebook Ireland Limited*, Handelsgericht Wien, 31 July 2014, p. 30.

<sup>92</sup> Article 29 Working Party Opinion 2/2010 on online behavioural advertising, WP171, 22 June 2010, p. 15.

<sup>93</sup> Cf. *supra*; Chapter 2 “Consent”.

<sup>94</sup> Cf. *infra*; Section 7.B “Sponsored Stories” and “social ads”.

<sup>95</sup> Cf. *infra*; Chapter 6 “Location Data”

As explained earlier, default settings which are configured to disclose information without the active engagement of the user do not constitute unambiguous consent.<sup>96</sup> When certain settings - not crucial to use the service - “overshare” data by default, a service provider cannot rely on the acceptance of its general terms and conditions or privacy policy in order to legitimate the processing at issue.<sup>97</sup>

Finally, it is worth noting that “privacy-unfriendly” default settings also raise questions from a **consumer law** perspective. It can be argued that such settings constitute unfair commercial practices.<sup>98</sup> When, in addition, these settings are well hidden and/or hard to adjust, they may also be qualified as “misleading”.<sup>99</sup> In relation to Facebook’s opt-out mechanism for online behavioural advertising, EDRI has noted that some of the language used to instruct users could be misleading and confusing.<sup>100</sup> Specifically, in one announcement regarding its revised Terms of Use, Facebook stated that:

*“That’s why Facebook respects the choices you make about the ads you see, across every device. You can opt out of seeing ads on Facebook based on the apps and sites you use through the Digital Advertising Alliance”.*<sup>101</sup>

According to EDRI, the quoted text gives the impression that users can opt out of data collection across every device by following the link to the Digital Advertising Alliance (DAA).<sup>102</sup> However,

*“The first sentence refers to the options (not linked to on the page) available inside Facebook’s service to opt out of advertising based on profiling (but not data collection for that purpose). The second sentence refers to something entirely different, a centralised opt-out process for a range of companies. Opting out through the DAA does not opt the user out across every device it operates, despite the fact that many DAA members take pride in their ability to follow users across devices.”*<sup>103</sup>

---

<sup>96</sup> Cf. *supra*; Chapter 2.

<sup>97</sup> See also Dutch Data Protection Authority (College Bescherming Persoonsgegevens), *Investigation into the combining of personal data by Google, Report of Definitive Findings*, November 2013, p. 5 and 83.

<sup>98</sup> Art. 8 Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’ or UCPD), Official Journal of the European Union, no L 149, 11 June 2005, 22-39 Directive 2005/29 is implemented in Belgian Law through Book VI of the BCEL.

<sup>99</sup> See art. 6-7 Unfair Commercial Practices Directive; article VI.97 BCEL.

<sup>100</sup> J. McNamee, Facing a challenge – understanding Facebook’s opt-out instructions, 11 February 2015, <https://edri.org/facing-challenge-understanding-facebooks-opt-out-instructions/>. (last accessed 25 March 2015).

<sup>101</sup> Facebook, “Updating Our Terms and Policies: Helping You Understand How Facebook Works and How to Control Your Information”, accessible at <https://www.facebook.com/about/terms-updates> (last accessed 25 March 2015).

<sup>102</sup> J. McNamee, Facing a challenge – understanding Facebook’s opt-out instructions, 11 February 2015, <https://edri.org/facing-challenge-understanding-facebooks-opt-out-instructions/>. (last accessed 25 March 2015).

<sup>103</sup> *Id.*

## 4. Unfair contract terms

The terms of use of OSNs are subject to the requirements of the Directive on unfair terms in consumer contracts (UCTD)<sup>104</sup>, as implemented into national laws.<sup>105</sup>

The UCTD prohibits the use of certain contractual terms. It contains a list of terms which may be regarded as “unfair” (annex 1), as well as a “catch-all” provision, which states that

*“a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer.”<sup>106</sup>*

Facebook’s SRR contains a number of provisions which, according to our analysis<sup>107</sup>, violate the UCTD. While these violations were already present in 2013, they are set to persist in 2015.

### A. Excessive linking

When registering for a Facebook account, the relevant webpage indicates that by clicking “Create an account”, they are agreeing to the SSR and that they have read Facebook’s Data Policy, including its Cookie Use Policy. These documents are not presented in full at the time of registration. Instead, individuals must access them by clicking a hyperlink:

---

<sup>104</sup> Council Directive (EC) 93/13 on unfair terms in consumer contracts [1993] *O.J.* 24 April 1993, L 95/29 (“UCTD”); <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0013&from=EN>. The UCTD is transposed into Belgian law in Book VI of the Code of Economic Law of 28 February 2013 (*B.S.*, 29 March 2013) (hereafter: “BCEL”).

<sup>105</sup> According to the European Commission’s Cloud Expert Working Group, the scope of the Unfair Contract Terms Directive 93/13/EEC is sufficiently broad to cover “free” services (“*The Unfair Contract Terms Directive has a broad scope and applies to all consumer contracts for the supply of goods and services. Furthermore, its application is irrespective of whether the consumer paid a monetary price or not as a counter performance. Thus, contracts for the supply of ‘free’ cloud computing services are covered as well*”) (European Commission’s Expert Group on Cloud Computing Contracts, “Unfair Contract Terms in Cloud - Computing Service Contracts - Discussion Paper”, p. 1, accessible at [http://ec.europa.eu/justice/contract/files/expert\\_groups/unfair\\_contract\\_terms\\_en.pdf](http://ec.europa.eu/justice/contract/files/expert_groups/unfair_contract_terms_en.pdf), last accessed 17 October 2014). See also M.B.M Loos and J.A. Luzak, “Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers”, *Amsterdam Law School Legal Studies Research Paper No. 2015-01 / Centre for the Study of European Contract Law Working Paper No. 2015-01*, accessible at <http://ssrn.com/abstract=2546859>.

<sup>106</sup> Article 3(1) UCTD.

<sup>107</sup> For a more extensive analysis see E. Wauters, E. Lievens and P. Valcke, “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* 2014, Vol. 22, No. 3, 254-294

# Create an account

It's free and always will be.

## Birthday

[Why do I need to provide my date of birth?](#)

Female

Male

By clicking Create an account, you agree to our [Terms](#) and that you have read our [Data Policy](#), including our [Cookie Use](#).

Create an account

The SRR contains references to other documentation, including Facebook's "Data Policy", the "Facebook Principles", the list of "Facebook Services", "Community Standards", "Platform Page", etc. The SRR contains a total of 30 hyperlinks which refer to 16 different pages, each of which typically contains one or more hyperlinks to other pages. Facebook's Data Use Policy contains a total of 26 hyperlinks which refer to 18 different pages, each of which typically contains one or more hyperlinks to other pages.

Article 5 of the UCTD provides that "in the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language."<sup>108</sup> The requirement of clarity contained in article 5 UCTD deals not only with substance but also with form.<sup>109</sup> In a case involving the terms of use of a low-cost airline, a Belgian Court ruled that the provisions were not clear and easy accessible and therefore violated article VI.37 §1 of the Code of Economic Law.<sup>110</sup> The judge concluded that the website in question displayed five major defects:

1. On the website, there are no complete Terms of Use to be found or another document that is fully exhaustive;
2. The technique of cross-referencing is too frequent and not very legible;

<sup>108</sup> See also article VI.37 §1 BCEL.

<sup>109</sup> Kh. Namen (3e k.) nr. A/09/00549, 10 March 2010, DCCR 2011, afl. 92-93, 146, note Reinhard Steennot.

<sup>110</sup> "When all of certain provisions of an agreement between a company and a consumer are in writing, they have to be drafted in a clear and comprehensible manner" (authors own translation).

3. There are no clear and precise rules for clarifying the hierarchy between the different texts;
4. In the section “Frequently Asked Questions” there are practicalities as well as essential conditions of the contract;
5. The lack of clarity results from the structure of the website and the consumer does not have the possibility to have the full knowledge of the Terms of Use.<sup>111</sup>

In its 2014 Recommendation regarding terms of use for social networks, the French Commission for abusive clauses (*Commission des clauses abusives*, CCA) also stated that the use of hyperlinks or of clauses that refer to each other can, when excessive, create a significant imbalance.<sup>112</sup>

## **B. Characterisation as a “free” service**

Facebook advertises its service as free: “*It’s free and always will be*”. The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – VZBV) has argued that this statement is misleading. While users do not pay a pecuniary fee, Facebook uses personal data of its users to sell personalised advertising space to advertisers.<sup>113</sup> According to the VZBV, individuals should be made aware of Facebook’s business model and of the importance of their personal data.<sup>114</sup>

A similar opinion was expressed by the French CCA in its 2014 Recommendation, where it noted that many social network providers give their users the impression that no compensation is necessary.<sup>115</sup> According to the CCA, however, the compensation lies in the use of the personal data and content of users. The CCA concluded that statements suggesting the social networking service is “free” constitute a “significant imbalance” between the rights and obligations of the contracting parties.<sup>116</sup>

---

<sup>111</sup> Kh. Namen (3e k.) nr. A/09/00549, 10 March 2010, DCCR 2011, afl. 92-93, 146, note Reinhard Steennot.

<sup>112</sup> See CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, paragraph 7 accessible at [www.clauses-abusives.fr/recom/index.htm](http://www.clauses-abusives.fr/recom/index.htm) (last accessed 28 May 2015).

<sup>113</sup> <http://www.vzbv.de/pressemeldung/facebook-fuehrt-nutzer-die-irre>

<sup>114</sup> <http://www.vzbv.de/pressemeldung/facebook-fuehrt-nutzer-die-irre>.

<sup>115</sup> CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, paragraph 14.

<sup>116</sup> Id.

## C. Warranty disclaimer

Clause 15(3) of Facebook's SRR disclaims any warranty for the content and the software:

*"We try to keep Facebook up, bug-free and safe, but you use it at your own risk. We are providing Facebook as is without any express or implied warranties including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections"*

The UCTD prohibits terms "*inappropriately excluding or limiting the legal rights of the consumer [...] in the event of non-performance or inadequate performance*".<sup>117</sup> The **blanket warranty disclaimer** contained in Facebook's SRR arguably violates this prohibition. In addition, the warranty disclaimer could also be invalidated under the catch-all provision of the UCTD (significant imbalance).<sup>118</sup>

According to the French Commission des Clauses Abusives (CCA), warranty disclaimers that do not give the right to reparation for consumers in the event of non-fulfilment by the business of any of its obligations, are presumed to be unlawful.<sup>119</sup>

## D. Liability limitation

Clause 15(3) of Facebook's SRR stipulates that

*"Our aggregate liability arising out of this statement or Facebook will not exceed the greater of one hundred dollars (\$100) or the amount you have paid us in the past twelve months."*<sup>120</sup>

There are two reasons to question the validity of this term. First, the UCTD consumer protection law prohibits companies from excluding liability for intentional or gross misconduct (cf. *supra*; Warranty disclaimer).<sup>121</sup> In addition, Facebook's liability cap of \$100 creates a **significant imbalance between the liability exposure of Facebook and that of its users**, which is, in principle, unlimited according to the same SRR (cf. *infra*; indemnity clause).

Clause 15(3) of Facebook's SRR further stipulates that

---

<sup>117</sup> UCTD, Annex 1 (b); Article VI.83, 13° BCEL.

<sup>118</sup> When assessing the fairness of a warranty clause, courts usually take into account the price paid for goods or services. If one accepts that a user "pays" with personal information, it could be argued that such a provision does cause an insignificant imbalance since the user "*gives up a significant amount of personal information in exchange for which he receives no guarantee of conformity of the goods or services.*" (IDATE, TNO and IVIR, User-Created-Content: Supporting a participative Information Society – Final report (2008) [http://www.ivir.nl/publications/helberger/User\\_created\\_content.pdf](http://www.ivir.nl/publications/helberger/User_created_content.pdf), p. 257.

<sup>119</sup> See CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, paragraphs 39-40 accessible at [www.clauses-abusives.fr/recom/index.htm](http://www.clauses-abusives.fr/recom/index.htm) (last accessed 18 March 2015).

<sup>120</sup> Article 16(3) of Facebook's "Statement of Rights and Responsibilities", 15 November 2013, accessible at <https://www.facebook.com/legal/terms> (last accessed 25 November 2014)

<sup>121</sup> UCTD, Annex 1 (b); Article VI.83, 13° BCEL. See also I. Samoy, P. Valcke, S. Janssen a.o., "Facebook maakt privéberichten openbaar: een casus contractuele aansprakelijkheid?", *l.c.*, p. 11.



*“Facebook is not responsible for the actions, content, information, or data of third parties, and you release us, our directors, officers, employees and agents from any claims and damages, known and unknown, arising out of or in any way connected with any claim you have against any such third parties.”*

According to the French CCA, clauses which seek to limit the liability of an OSN for actions which would otherwise give rise to liability (e.g., failure to act promptly in case of manifestly illegal content upon notice) are unlawful.<sup>122</sup>

## **E. Indemnity clause**

Clause 15(2) of Facebook’s SSR stipulates that

*“If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.”*

This clause essentially obliges users to indemnify Facebook for any expenses incurred, including legal fees, as a result of any action, content or information on Facebook. The validity of such clauses has been contested as being unfair.<sup>123</sup> Moreover, under Belgian law, the recoverability of legal fees is governed by article 1022 the Code of Civil Procedure.<sup>124</sup> This law limits the amount of damages that can be recuperated for legal expenses in disputes between private parties. In principle, no one may be asked to reimburse legal expenses above the maximum amounts established by Royal Decree (article 1022 *in fine* of the Belgian Code of Civil Procedure).<sup>125</sup>

As for other damages, Facebook would need to demonstrate the existence of a direct causal relationship between the infringement of the third-party rights by the Facebook user and the damages suffered by Facebook. Very often, the actual liability exposure of an OSN provider for user-generated content results not only from the content itself, but from its own failure to act. A distinction therefore needs to be made between the action of the user and the non-action of the

---

<sup>122</sup> See CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, l.c., paragraph 27.

<sup>123</sup> For example, in 2004, a consumer organisation successfully challenged a “hold harmless” provision included in the terms of use of internet service provider AOL France. See Tribunal de Grande Instance de Nanterre (1ère chambre), *UFC Que Choisir / AOL Bertelsmann Online France*, 2 June 2004, paragraph 13, accessible at [http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=1211](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1211). In a guidance document on these Regulations the Office of Fair Trading in the UK also indicated that such an indemnity clause may be unfair: OFT, ‘Unfair contract terms guidance. Guidance for the Unfair Terms in Consumer Contracts Regulations 1999’ (2008), [http://www.offt.gov.uk/shared\\_offt/reports/unfair\\_contract\\_terms/oft311.pdf](http://www.offt.gov.uk/shared_offt/reports/unfair_contract_terms/oft311.pdf).

<sup>124</sup> Article 1022 of the Code of Civil Procedure was modified in 2007 in order to provide for the recoverability of legal fees Wet van 21 april 2007 betreffende de verhaalbaarheid van de erelonen en de kosten verbonden aan de bijstand van een advocaat, B.S. 31 mei 2007).

<sup>125</sup> Koninklijk besluit van 26 oktober 2007 tot vaststelling van het tarief van de rechtsplegingsvergoeding bedoeld in artikel 1022 van het Gerechtelijk Wetboek en tot vaststelling van de datum van inwerkingtreding van de artikelen 1 tot 13 van de wet van 21 april 2007 betreffende de verhaalbaarheid van de erelonen en de kosten verbonden aan de bijstand van de advocaat.

OSN provider. Any attempt to hold OSN users liable for the fault of the OSN provider may be considered unfair and therefore invalid.<sup>126</sup>

## F. Unilateral change

Facebook reserves the right to change their SRR and DUP unilaterally:

*“We’ll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services.*

*If we make changes to policies, guidelines or other terms referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.*

*Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines”*

The UCTD stipulates that a term may be unfair when it enables a “seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract.”<sup>127</sup> This provision of the UCTD has been implemented differently across Member States. In Belgium, the Code of Economic Law provides that a unilateral change clause may not deprive consumers of the ability to end the contract before these new conditions apply, without extra costs and without compensation.<sup>128</sup>

It is interesting to note that a German court has invalidated this provision of Facebook’s SRR because of its “significant imbalance”.<sup>129</sup> According to the Court, provisions which allow the company or trader to change the terms without the consent of the consumer, are only permitted when they are restricted to remedy “equivalence problems”<sup>130</sup> and gaps in the conditions, and if they are drafted in a clear manner. Facebook, however, grants itself seemingly unlimited power to amend the terms. The notice period and the possibility to participate under certain conditions

---

<sup>126</sup> See also M.B.M Loos and J.A. Luzak, “Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers”, *l.c.*, p. 18. See also CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, *l.c.*, paragraph 38, in which the CCA finds that these kind of provisions creates a significant imbalance in the parties, because of their nature general, they are not limited solely to the case of the fault of the user and the repair of its consequences.

<sup>127</sup> UCTD, Annex 1 (j)

<sup>128</sup> Article VI.83, 2° BCEL.

<sup>129</sup> Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <http://openjur.de/u/269310.print>.

<sup>130</sup> The interest of each party lies in the value of a corresponding return for its performance. For instance, person A and B conclude an agreement concerning a purebred dog. Person A pays a price that is common for purebred dogs. However, if afterwards it turns out that the dog is of a mixed breed, the equivalence of person A is disturbed because he has not received the full benefits of the price he paid (see <http://www.lexexakt.de/glossar/aequivalenzinteresse.php>).

softened the power of unlimited amendment, but this does not, according to the Court, alter the fact that the amendment provision violates German Law.<sup>131</sup>

## G. Forum clause

Clause 15(1) of Facebook's 2015 SRR provides that

*"You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims."*

Within the EU, disputes with a cross-border element are subject to the Brussels I Regulation<sup>132</sup>, which lays down the rules for jurisdiction and enforcement in civil and commercial matters.

Article 17(1)c of Brussels I provides that the rules concerning jurisdiction over consumer contracts shall apply if

*"the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities."*

Article 17(2) of Brussels I goes on to specify:

*"Where a consumer enters into a contract with a party who is not domiciled in the Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that State."*

Facebook has offices in the EU (including Ireland, Belgium, the Netherlands and Germany). As a result, they can be considered to have a "branch, agency or other establishment" in these Member

---

<sup>131</sup> Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <<http://openjur.de/u/269310.print>> accessed 9 September 2013, last accessed 9 September 2013. See also CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, l.c., paragraph 33, where the CCA states that unilateral changes and the presumption of consent are deemed to be abusive under French consumer law.

<sup>132</sup> Regulation (EU) no 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. 2012, L 351/1 (hereafter: "Brussels I"). This Regulation applies as of 10 January 2015 (art. 81). Before January 10 2015, these matters were regulated Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ 2001, L 12/1 (which contained very similar provisions). See also M.B.M Loos and J.A. Luzak, "Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers", l.c., p. 19.

States within the meaning of article 17(2) of Brussels I.<sup>133</sup> In any event, Facebook also “directs” its activities to these Member States within the meaning of article 17(c).

Article 18 (1) of Brussels I offers consumers the choice of either bringing proceedings in the courts in the Member State where he is domiciled or in the Member State where the other party is domiciled.<sup>134</sup> In contrast, the consumer can only be sued in the Member State where he is domiciled.<sup>135</sup> Parties can only deviate from this after a dispute has arisen and only under certain conditions.<sup>136</sup> This implies that the **forum clause of Facebook’s SSR is invalid**.<sup>137</sup>

In addition to the Brussels I Regulation, it is also important to take into account the UCTD when assessing a jurisdiction clause. In *Océano*, the CJEU concluded that

*“where a jurisdiction clause is included, without being individually negotiated, in a contract between a consumer and a seller or supplier within the meaning of the Directive and where it confers exclusive jurisdiction on a court in the territorial jurisdiction of which the seller or supplier has his principal place of business, it must be regarded as unfair within the meaning of Article 3 of the Directive in so far as it causes, contrary to the requirement of good faith, a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer.”*<sup>138</sup>

---

<sup>133</sup> One might argue that disputes concerning Facebook’s SRR or DUP do not directly “arise out of the operations of the branch, agency or establishment” established in the EU, as the relevant decisions are made by Facebook headquarters, which are located in California. However, given that the operations of Facebook’s European offices are “inextricably linked” to those of Facebook’s primary establishment, one may argue that disputes regarding Facebook’s DUP or SRR do in fact also arise out of the operations of the branch, agency or establishment. For an analogous reasoning see CJEU, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, 13 May 2014, at paragraphs 47 et seq.

<sup>134</sup> See also M.B.M Loos and J.A. Luzak, “Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers”, *l.c.*, p. 20.

<sup>135</sup> Article 18(2) Brussels I Regulation.

<sup>136</sup> See article 19 of the Brussels I Regulation. See also P. A. Nielsen, ‘Art. 17’ in Ulrich Magnus and Peter Mankowski *Brussels I Regulation* (Sellier European Law Publishers, München 2007), 321; G. Mazziotti, *EU Digital Copyright Law and the End-User* (Springer, Berlin Heidelberg, 2008), 122; Susan Schiavetta, Does the Internet Occasion New Directions in Consumer Arbitration in the EU? (2004) 3 JILT, 2004, accessible at [http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004\\_3/schiavetta](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/schiavetta).

<sup>137</sup> See also M.B.M Loos and J.A. Luzak, “Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers”, *l.c.*, p. 20. See also Tribunal de grande instance de Paris, Frédéric X. / Facebook Inc., 5 March 2015, 4ème chambre – 2ème section, accessible at [http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=4515](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4515).

<sup>138</sup> CJEU, Joined cases C-240/98 to C-244/98 *Océano Grupo Editorial SA v Roció Murciano Quintero, Salvat Editores SA v José M. Sánchez Alcón Prades, José Luis Copano Badillo, Mohammed Berroane and Emilio Viñas Feliú* [2000] ECR I-4941, para 24. See also Ulrich Magnus and Peter Mankowski, *Brussels I regulation, European commentaries on private international law* (Sellier European Law Publishers, München 2007), 322 M.B.M Loos and J.A. Luzak, “Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers”, *l.c.*, p. 20 and See CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, *l.c.*, paragraph 44.

## H. Choice of law

According to Clause 15(1) Facebook's SRR, any disputes relating to the SRR or Facebook shall be governed by Californian Law. However, article 6 of Regulation No 593/2008 (Rome I)<sup>139</sup> provides that consumer contracts shall in principle be governed by the law of the country where the consumer has his habitual residence. While parties may choose for a different law to be applicable under certain conditions, such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable (article 6(2) of Rome I).<sup>140</sup>

The French Commission for abusive clauses (CCA) has indicated that choice of law clauses with contents similar to Clause 15(1) of Facebook's SRR create a **significant imbalance** in the parties, because they give the impression that consumers cannot benefit from the protection of French law, although the latter is more protective than the law referred to in the provision.<sup>141</sup>

## I. Termination

Clause 14 of Facebook's SSR provided that:

*If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: (...)*

Under the UCTD, terms that enable "*the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so*" may be unfair.<sup>142</sup> Given the differences in transposition of the Unfair Terms Directive in Member States, the latter will have to be judged on a country-specific basis. For instance, Germany has not implemented this provision in its national law as such.<sup>143</sup> In Belgium, the provision is part of a "black list"<sup>144</sup>, which provides that any provision which "[...] *authorizes a company to terminate*

---

<sup>139</sup> Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), *O.J. L-177*, 4 July 2008, 6-16.

<sup>140</sup> See also I. Samoy, P. Valcke, S. Janssen a.o., "Facebook maakt privéberichten openbaar: een casus contractuele aansprakelijkheid?", *Juristenkrant* 5 December 2012, p. 10; E. Wauters, E. Lievens, P. Valcke and K. Lefever, "Over Tweeten, Friends & Followers: Juridische Kijk op Sociale Media", in P. Valcke en J. Dumortier (eds.), *ICT- en Mediarecht*, Brugge; Die Keure, 2012, p. 5-6 and See also M.B.M Loos and J.A. Luzak, "Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers", *l.c.*, p. 22-23.

<sup>141</sup> CCA, Recommendation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, *l.c.*, at paragraph 46.

<sup>142</sup> Annex article 1 (g) Unfair Terms Directive.

<sup>143</sup> M. Skory, *Study: Abusive clauses – application of the provisions of Directive 93/13 in Poland and selected countries of the European Union (Germany, Great Britain, France, the Czech Republic, Slovakia and Hungary)* (2007), 22.

<sup>144</sup> A blacklist is a list of clauses which are considered to be absolutely unlawful. H.W. Icklitz, J. Stuyck and E. Terryn (eds), *Cases, Materials and Text on Consumer Law*, (Hart, Oxford/Portland 2010), 291.

*an agreement of indefinite time period without a reasonable notice period*” shall be **unlawful** (except in case of “force majeure”).<sup>145</sup> In France, the French CCA has indicated that termination clauses in social networking contracts which do not provide for a reasonable notice period create a significant imbalance between the parties.<sup>146</sup>

Although Germany has not transposed the provision directly, a German court<sup>147</sup> has already invalidated Facebook’s termination clause because it provides an extraordinary right of termination since it does not provide a warning or a valid reason. The provision was considered to be in breach with the core of article §314 of the German Civil Code (*Bürgerliches Gesetzbuch*), which stipulates that each party can end a contract without a notice period when there is a compelling reason.<sup>148</sup> If the compelling reason constitutes a breach of duty under the contract, it can only be ended after the expiration of a relief period in which no solution was found or when a warning was issued to the party who breached the contract and did not respond to this warning.<sup>149</sup>

Facebook’s termination provision is very broad and very general, making it difficult for users to know when they risk seeing their account suspended. Facebook has a history of using many different reasons to disable accounts, such as “*not using your real name, posting offensive content, scraping the site, joining too many groups, sending too many messages, ‘poking’ too many people, or sending the same message too many times.*”<sup>150</sup> People using their real names have seen their accounts being disabled without warning or recourse because Facebook found they were in breach of their real name policy.<sup>151</sup> In addition, reasons such as “sending too many messages” are inherently subjective. What may seem an extensive amount of messages to one person, may be considered absolutely normal by another person.

---

<sup>145</sup> Art. VI.83 11° BCEL. See also R. Steennot, Commentaar bij art. 74, 11° wet 6 april 2010, X., Handels- en economisch recht. Commentaar met overzicht van rechtspraak en rechtsleer, X. Marktpraktijken, 1-2.

<sup>146</sup> CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, *l.c.*, at paragraph 36.

<sup>147</sup> Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <http://openjur.de/u/269310.print>.

<sup>148</sup> The law speaks of a “compelling reason” if the party who ends the contract, after taking all circumstances of the specific case into account and weighing the interests of both parties, cannot be reasonably expected to continue the contract until the agreed end or until the expiration of a notice period.

<sup>149</sup> See article §314 Bürgerliches Gesetzbuch.

<sup>150</sup> Eric Schonfeld, ‘Facebook Stirring Up Anger For Disabling Accounts’, *Techcrunch* (11 July 2007) <<http://techcrunch.com/2007/12/11/facebook-stirring-up-anger-for-disabling-accounts>> accessed 9 September 2013.

<sup>151</sup> Asher Moses, ‘Banned for keeps on Facebook for odd name’, *The Sydney Morning Herald* (25 September 2008) <http://www.smh.com.au/news/biztech/banned-for-keeps-on-facebook-for-odd-name/2008/09/25/1222217399252.html>.

## 5. How Facebook “combines” and “shares” data about its users

As indicated in the introduction, Facebook brings together information about its users from a wide variety of sources. The main purpose of this section is to illustrate some of Facebook’s current practices by presenting **three use cases**. The first two use cases (“*Custom Audiences*” and “*Lookalike audiences*”) illustrate how Facebook combines personal data received from third-parties (advertisers) with the data it has about its own users. The third use case (*Atlas*) illustrates how Facebook combines and/or shares data across Facebook services and companies.

### A. Custom Audiences

Custom Audiences is an advertising feature which allows advertisers “to reach customers [they] already know with ads on Facebook.”<sup>152</sup> Specifically, it allows advertisers to use information which has been collected outside of Facebook in order to target individuals with ads on Facebook. Custom Audiences **can be created in three different ways**:

- (1) on the basis of a “Customer List”;
- (2) on the basis of “Website Traffic” (pixel tracking); or
- (3) on the basis of “App Activity”.

The following screenshots illustrate the process for creating a Custom Audience using Facebook Ads Manager<sup>153</sup>:

#### Custom Audiences

Connect with the people who have already shown an interest in your business or product with Custom Audiences. You can create an audience from your customer contacts, website traffic or mobile app.

Create a Custom Audience

An advertiser who decides to create a Custom Audience, will be prompted to select the method by which it would like to create a Custom Audience:

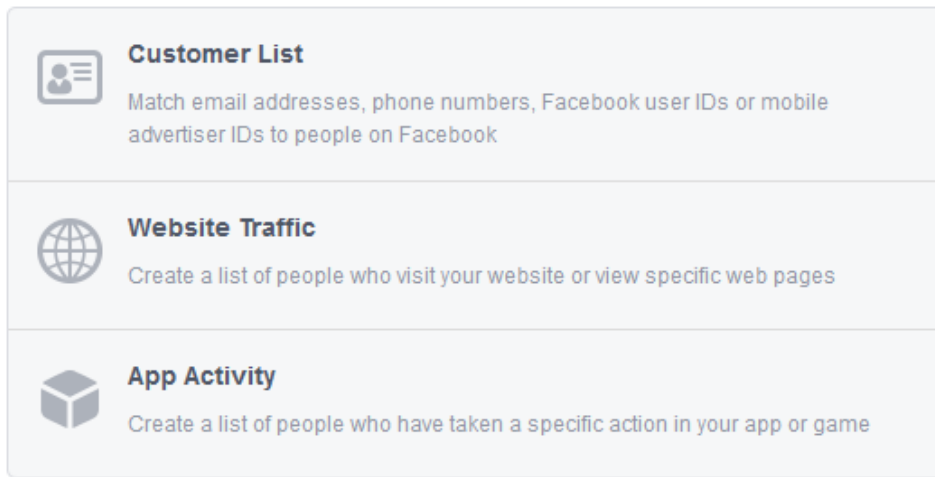
---

<sup>152</sup> Facebook, “What is a custom audience?”, <https://www.facebook.com/help/341425252616329> (last accessed 24 August 2015). Custom Audiences became available to all advertisers in October 2013: see Facebook, “Custom Audiences is now available to every advertiser”, *Facebook for business*, 23 October 2013, <https://www.facebook.com/business/news/Custom-Audiences-Is-Now-Available-to-Every-Advertiser> (last accessed 24 August 2015).

<sup>153</sup> Custom audiences can also be created using “Ad creation”; “Power Editor” and “Analytics for Apps”. See also Facebook, “How Do I Create a Custom Audience?” <https://www.facebook.com/help/170456843145568> (last accessed 19 August 2015).

## Choose the type of audience you want to create on Facebook.

This process is secure and the details about your customers will be kept private.



The screenshot shows three options for creating an audience on Facebook:

- Customer List**: Match email addresses, phone numbers, Facebook user IDs or mobile advertiser IDs to people on Facebook
- Website Traffic**: Create a list of people who visit your website or view specific web pages
- App Activity**: Create a list of people who have taken a specific action in your app or game

### 1) Customer List

An advertiser who chooses the option “Customer List”, will be prompted to share a list of email addresses, phone numbers, Facebook user IDs or mobile advertiser IDs with Facebook. The advertiser can either (a) upload a .csv or .txt file; (b) import a customer list from a third-party mail service (MailChimp); or (c) simply copy paste the list, as shown in the image below:

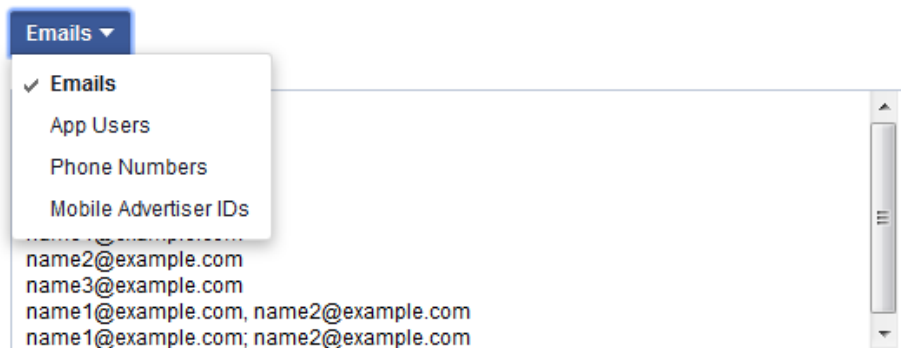


#### Copy and paste your customer list

Copy and paste a list of email addresses, phone numbers, Facebook user IDs or mobile advertiser IDs from a spreadsheet or text file.

You can copy columns from a spreadsheet with one record per row or a list of records separated by commas. [View formatting examples.](#)

#### Data Type



The screenshot shows a dropdown menu for selecting the data type. The menu is open, showing the following options:

- ✓ Emails
- App Users
- Phone Numbers
- Mobile Advertiser IDs

Below the dropdown menu, there is a text input field containing the following text:

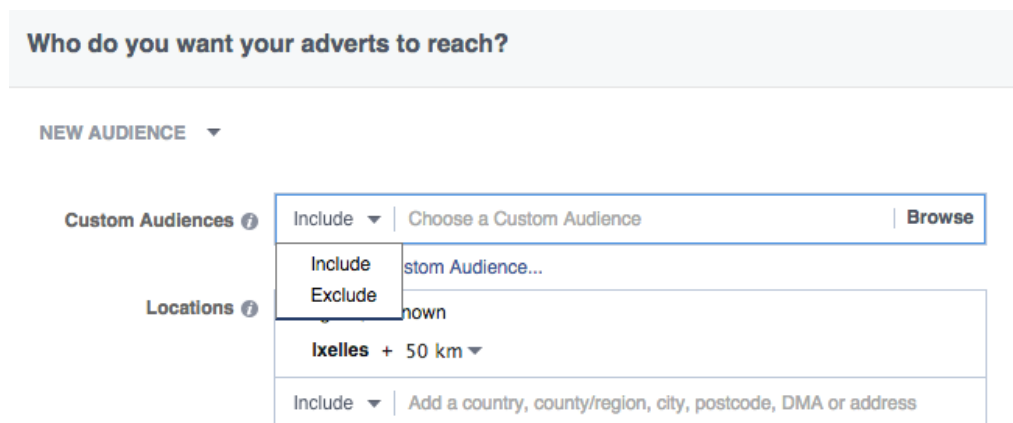
```
name2@example.com  
name3@example.com  
name1@example.com, name2@example.com  
name1@example.com; name2@example.com
```



According to Facebook’s promotional video for Custom Audiences, customer contact information “is always used in a secure, anonymous, privacy-safe way”.<sup>154</sup> Presumably this statement refers to Facebook’s stated practice of hashing customer list entries before being sent to Facebook:<sup>155</sup>

1. Facebook hashes the email addresses and phone numbers our users have provided us. You begin uploading your customer list and it is hashed locally in your browser before it's uploaded to Facebook.
2. After your hashed data is uploaded to Facebook, we match it against ours.
3. The matches are added to a Custom Audience for you.
4. The matched and unmatched hashes are deleted.

Once the Custom Audience has been created, the Advertiser will be able to **either target or exclude** the “matched” individuals in future advertising campaigns on Facebook. For example, an advertiser might create a list of email addresses of its “low budget” customers, and convert it into a Custom Audience “A”. The advertiser could then choose to either target or exclude individuals belonging to Custom Audience A during a particular advertising campaign on Facebook.



<sup>154</sup> See Facebook for business, “Target Facebook Adverts to people on your contact list”, <https://www.facebook.com/business/a/custom-audiences> (last accessed 24 August 2015)

<sup>155</sup> Facebook, “What happens when I upload my customer list to Facebook”, <https://www.facebook.com/help/112061095610075> (last accessed 24 August 2015).

## 2) Website traffic

“Website traffic” is a targeting option that allows advertisers to target Facebook users who have previously visited their website.<sup>156</sup> It is described by Facebook as *“a powerful way to reach existing customers and those who’ve shown some interest in your business before”*.<sup>157</sup>

To use this targeting option, the advertiser must first install a so-called **“Custom Audience Pixel”** on its website.<sup>158</sup> Once the pixel has been installed, the advertiser will be able to automatically target advertisements to any Facebook user who visits the webpage(s) where the pixel was installed.<sup>159</sup>

### Create a custom audience from your website

Show adverts to people who visit your website.

You can set up your audience to include everyone who visits your website, or even create separate audiences for people who visit specific pages on your website.

Install the Custom Audience pixel on your website to start building your audience automatically. You can also send this code directly to the person who manages your website.

Advertisers are encouraged to place the pixel code *“anywhere on [their] website where [they] would like to identify people”*.<sup>160</sup>

### View Custom Audience Pixel

Copy the code below and paste it between <head> and </head> in your website code. Then you can set up rules to track specific actions that people take across your website.

Send the code to your website developer

```
<script>(function() { var _fbq = window._fbq || (window._fbq = []); if (!_fbq.loaded) { var fbd
```

---

<sup>156</sup> Facebook, “What are Custom Audiences from your website?”, <https://www.facebook.com/help/610516375684216> (last accessed 24 August 2015).

<sup>157</sup> Facebook, “Custom Audiences from your Website”, <https://www.facebook.com/help/449542958510885> (last accessed 24 August 2015).

<sup>158</sup> According to Facebook *“A Custom Audience pixel is a piece of JavaScript code that an advertiser can place on their website to create a website Custom Audience. The pixel is activated every time someone opens a web page where the code is installed. This piece of code sends this general, hashed, info about the actions people take on the website to Facebook to help the advertiser target their ads to the people who took an action on their website.* See Facebook, “What is a Custom Audience Pixel?” <https://www.facebook.com/help/742478679120153> (last accessed 24 August 2015).

<sup>159</sup> For more information see Facebook for business, “Custom Audiences from your website”, <https://www.facebook.com/business/a/online-sales/custom-audiences-website> (last accessed 24 August 2015).

<sup>160</sup> Facebook, “How does the Custom Audience pixel create an audience from my website?”, <https://www.facebook.com/help/454699474675736> (last accessed 24 August 2015).

Once the pixel code has been obtained, the advertiser must specify the “**rules**” that will trigger the Facebook pixel to identify the person on their website (e.g., “People who visit specific web pages” or “People visiting specific web pages but not others”).<sup>161</sup> When someone visits the webpage in question and matches against the criteria an advertiser has set, “a tracking cookie will be placed on that person and they’ll be added to [the advertiser’s] audience”.<sup>162</sup>

Advertisers who make use of an “Upgraded” Custom audience pixel are able to further adjust the **standard events** that trigger pixel tracking.<sup>163</sup> Standard events include (actual availability may vary):

- (1) “Key page view”;
- (2) “Search”;
- (3) “Add to cart”;
- (4) “Add to wish list”;
- (5) “Initiate checkout”;
- (6) “Add payment info”;
- (7) “Make purchase”;
- (8) “Lead”
- (9) “Complete registration”.<sup>164</sup>



The upgraded Custom Audience pixel code with a standard event<sup>165</sup>

<sup>161</sup> Facebook, “Can I customize my Custom Audience from my website depending on what pages people visit?”, <https://www.facebook.com/help/478163642285039> (last accessed 24 August 2015).

<sup>162</sup> Facebook, “How does the Custom Audience pixel create an audience from my website?”, <https://www.facebook.com/help/454699474675736> (last accessed 24 August 2015).

<sup>163</sup> Facebook, “The Upgraded Custom Audience Pixel” <https://www.facebook.com/help/952192354843755> (last accessed 24 August 2015).

<sup>164</sup> *Id.*

<sup>165</sup> *Id.*

### 3) App activity

“App activity” is a targeting option similar to “Website traffic”, but it is geared towards application providers instead of website operators. It allows application providers to target Facebook users with advertisements on the basis of the **actions they have taken (or not taken) within an application**.<sup>166</sup> For example, app providers can target people who previously used their app, but have not come back to the app within the last 90 days.<sup>167</sup> Or they can target people who have added an item to their cart in the app but did not make a purchase.<sup>168</sup>

To use this targeting option, the application provider must first register its app with Facebook and **integrate the Facebook SDK** (Software Development Kit)<sup>169</sup>:

#### Create a Custom Audience From Your App

Create a custom audience to reach people who take specific actions in your app - like reaching a specific level in a game, adding items to their cart or rating your app.

Start measuring events in your app by integrating our SDK for iOS, Android and Canvas. Every time someone takes the specified action within your app, they will be added to your Custom Audience.

Once the Facebook SDK has been installed and configured, the application provider will be able to specify the **App Events** it wishes to be “logged”.<sup>170</sup> App Events include<sup>171</sup>:

- (1) “Achieved level”
- (2) “Activated App”
- (3) “Added Payment Info”;
- (4) “Added to Cart”
- (5) “Added to Wishlist”
- (6) “Completed Registration”
- (7) “Completed Tutorial”
- (8) “Initiated Checkout”.

---

<sup>166</sup> Facebook for developers, “Targeting by App Activity”, <https://developers.facebook.com/docs/app-ads/targeting/by-app-activity> (last accessed 24 August 2015).

<sup>167</sup> *Id.*

<sup>168</sup> *Id.*

<sup>169</sup> For more information see Facebook for developers, “Targeting by App Activity”, <https://developers.facebook.com/docs/app-ads/targeting/by-app-activity> (last accessed 24 August 2015).

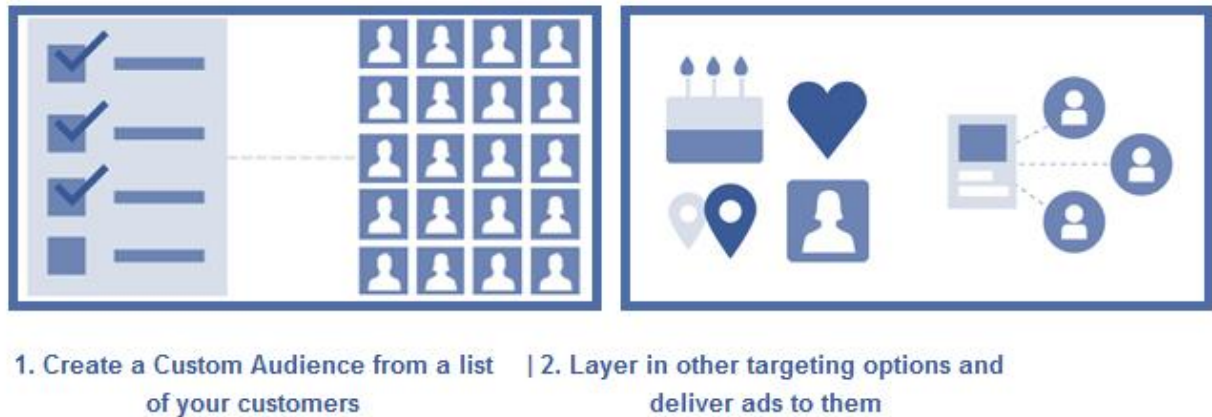
<sup>170</sup> See Facebook for developers, “AppEventsLogger”, <https://developers.facebook.com/docs/reference/android/current/class/AppEventsLogger> (last accessed 25 August 2015).

<sup>171</sup> Facebook for developers, “App Events for Android”, <https://developers.facebook.com/docs/app-events/android> (last accessed 25 August 2015).

Enabling “App Events” will also automatically allow the application provider to use Facebook Analytics for Apps.<sup>172</sup>

#### 4) Additional Facebook targeting options

Advertiser who have created a Custom Audience can further target their ads (i.e. “narrow down their Custom Audience”<sup>173</sup>) by using additional Facebook’s audience targeting options.<sup>174</sup>



The targeting options which Facebook provides include<sup>175</sup>:

- (1) “**Location**” (which allows advertisers to target “*Everyone in this location*”; “*People who live in this location*”; “*People recently in this location*” and “*People traveling in this location*”)<sup>176</sup>;

<sup>172</sup> See Facebook for developers, “Analytics for Apps”, <https://developers.facebook.com/docs/analytics> (last accessed 24 August 2015). It is worth noting that Facebook has recently announced a number of new services for app developers. Parse, for example, is an application development platform which enables developers to build apps but also to monitor their use by offering: “a single place to understand your app’s audience and measure how people use your app. This enables you to see the effectiveness of your ads, create better experiences for people in your app, and better understand the people who use your app through anonymized, aggregated insights.” In addition, app developers (or as Facebook calls them: “mobile app publishers”) will also be able to monetise the stream of users who visit their apps through LiveRail: “Mobile app publishers can now use LiveRail’s monetization platform to manage their video and display ads business. Additionally, LiveRail is enabling publishers to use Facebook’s approach for delivering the right ad to the right audience—meaning better results and better experiences for people.” (L. Deborah, “F8 2015: Using Facebook’s Family of Services to Build, Grow and Monetize Apps”, 25 March 2015, [https://developers.facebook.com/blog/post/2015/03/25/F8\\_2015\\_Roundup](https://developers.facebook.com/blog/post/2015/03/25/F8_2015_Roundup) (last accessed 24 August 2015).

<sup>173</sup> Facebook, “Can I use targeting to narrow down my Custom or Lookalike Audience?” <https://www.facebook.com/help/365659450209683> (last accessed 24 August 2015).

<sup>174</sup> Facebook, “Custom Audiences”, <https://www.facebook.com/help/381385302004628> (last accessed 24 August 2015).

<sup>175</sup> Facebook, “Audience Targeting Options”, <https://www.facebook.com/help/633474486707199> (last accessed 24 August 2015).

<sup>176</sup> Facebook, “What options do I have when selecting people within a location?”, <https://www.facebook.com/help/755086584528141> (last accessed 24 August 2015).

- (2) **“More demographics”** (which allows advertisers to target *inter alia* by education levels, specific schools, fields of study or specific graduation years)<sup>177</sup>;
- (3) **“Age & Gender”**<sup>178</sup>;
- (4) **“Interests”** (which allows advertisers to target on the basis of “*things people share on their Timelines, apps they use, Pages they like and other activities on and off of Facebook*”)<sup>179</sup>;
- (5) **“Behaviours”** (e.g., “device usage”, “purchase behaviours or intents”, “travel preferences”)<sup>180</sup>;
- (6) **“Connections”** (which allows advertisers to target “only people who have a connection with you”, “people who don’t have a connection with you”, “both of those groups”, or “friends of people who have a connection to you”)<sup>181</sup>.

The screenshot displays the Facebook targeting interface. On the left, the 'Custom Audiences' section is active, showing a search for 'KULEUVEN'. Below this, the 'Locations' section is set to 'Belgium' with 'All Belgium' selected. The 'Age' range is set to '18' to '65+', and 'Gender' is set to 'All'. The 'More Demographics' dropdown menu is open, listing categories such as Relationship, Education, Work, Home, Ethnic Affinity, Generation, Parents, Politics (US), and Life Events. On the right, the 'Audience Definition' section features a gauge showing the selection is 'fairly broad'. Below the gauge, 'Audience Details' are listed: Location: Belgium and Age: 18-65+. The 'Potential Reach' is stated as 5,300,000 people.

<sup>177</sup> Facebook, “How do I target education levels, specific schools, fields of study or specific graduation years?”, <https://www.facebook.com/help/227971680551772> (last accessed 24 August 2015).

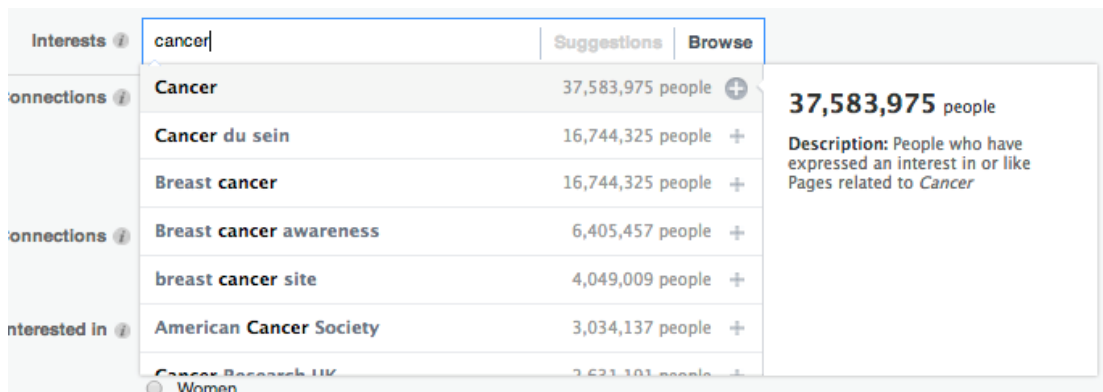
<sup>178</sup> Facebook, “Can I target my ad to people based on their age and gender?”, <https://www.facebook.com/help/813939365351532> (last accessed 24 August 2015).

<sup>179</sup> Facebook, “What is interests targeting?”, <https://www.facebook.com/help/188888021162119> (last accessed 24 August 2015).

<sup>180</sup> Facebook, “What are audience behaviors?”, <https://www.facebook.com/help/243268465859743> (last accessed 24 August 2015).

<sup>181</sup> Facebook, “What is connections targeting?”, <https://www.facebook.com/help/186282224754628> (last accessed 24 August 2015).

It is worth noting that the “Interests” targeting option makes it possible to target users with relation to potentially “sensitive” categories of information such as sexual orientation, political affiliation and medical information. Facebook describes “Interests” audience segments as “People who have expressed an interest or like pages related to X”, whereby X might for example refer to a medical condition, as shown in the following screenshot.



Interestingly, Facebook states that it does not allow advertisers to use sensitive personal data for purposes of ad targeting and that topics chosen by advertisers “don't reflect the personal beliefs, characteristics or values of users.”<sup>182</sup>

## B. Lookalike Audiences

Once an advertiser has set up a Custom Audience, the advertiser will also be able to target other Facebook users belonging to so-called “Lookalike Audiences”. Lookalike Audiences are audience segments defined by Facebook on the basis of **similarities** between the individuals included in a Custom Audience and **other Facebook users**.<sup>183</sup> Facebook creates Lookalike audiences on the basis of “common qualities” (e.g., demographic, interests) of people included in the source audience.<sup>184</sup> Lookalike audiences can be built on the basis of Customer Lists, Web traffic, App Activity, or from fans of a Facebook Page.<sup>185</sup>

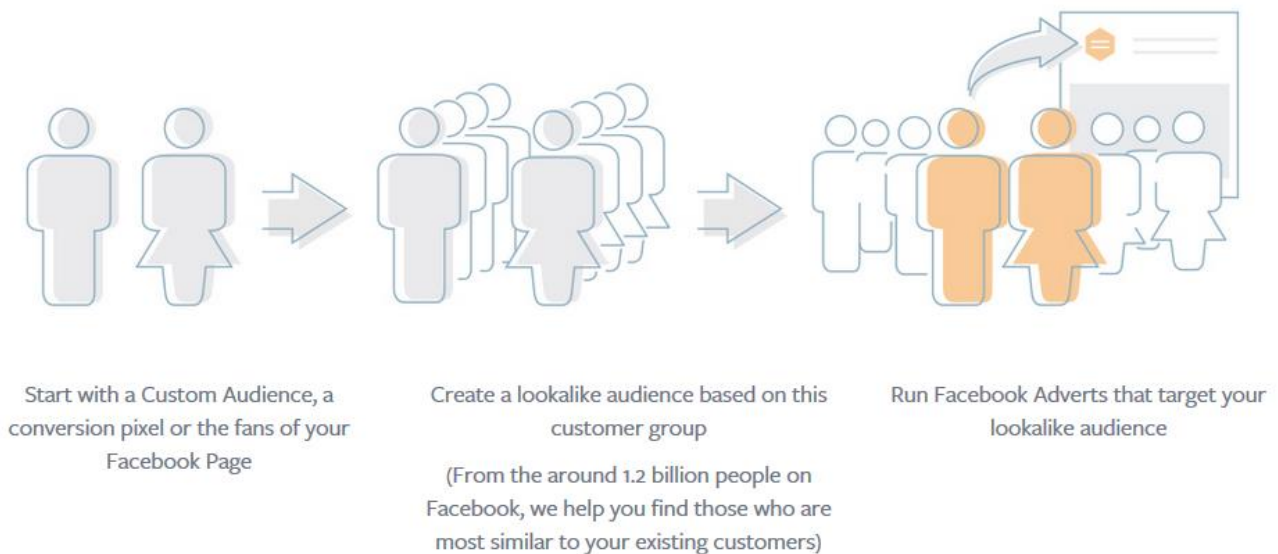
<sup>182</sup> Facebook, “Advertising Policies – Things you should know”, <https://www.facebook.com/policies/ads> (last accessed 25 August 2015). See also Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, l.c., p. 17-18.

<sup>183</sup> See Facebook for business, “Lookalike audiences”, <https://www.facebook.com/business/a/lookalike-audiences>; Facebook for business, “Finding People Similar to Your Customers”, <https://www.facebook.com/business/learn/facebook-ads-lookalike-audiences> and Facebook, “What are Lookalike Audiences?”, <https://www.facebook.com/help/164749007013531> (last accessed 24 August 2015).

<sup>184</sup> Facebook, “How does Facebook create my Lookalike Audience?” <https://www.facebook.com/help/1405191663080982> (last accessed 24 August 2015).

<sup>185</sup> Facebook, “What kinds of sources can I use to create a Lookalike Audience?”, <https://www.facebook.com/help/540208646002529>; Facebook, “Lookalike Audiences”,

## How lookalike audiences work



For example, an advertiser might create a list of email addresses of “big spender” customers, and convert it into a Custom Audience “A”. Facebook can then analyse the characteristics of the individuals in Custom Audience A and look for common patterns. Once Facebook’s algorithm has found similarities, it creates a larger segment of Facebook users that are similar (“look like”) the individuals included in Custom Audience “A” of the advertiser.<sup>186</sup> Once a Lookalike Audience has been created, the advertiser will be able to **either target or exclude** individuals included in the Lookalike audience in future advertising campaigns on Facebook.<sup>187</sup>

Advertisers that use Lookalike Audiences are also able to further “narrow down” their audience using Facebook’s additional targeting features described above.<sup>188</sup>

---

<https://www.facebook.com/help/231114077092092>; and Facebook for business, “Expanded Capabilities for Lookalike Audiences”, <https://www.facebook.com/business/news/Expanded-Capabilities-for-Lookalike-Audiences> (last accessed 24 August 2015).

<sup>186</sup> Very few details are available as to how exactly Lookalike Audiences are created by Facebook. A Facebook engineer has been quoted as saying: “When Facebook creates lookalike audiences from a custom audience, all kinds of features are considered. Age, sex, and location are factored in, but so are other things like likes, and interests. The automatic algorithm which creates the lookalike audience attempts to find common patterns among the audience [...]” (J. Muller, “Facebook Lookalikes: Do They Look Like They Should?”, Slum Digital Blog, 27 January 2014, <http://blog.sumdigital.com/facebook-lookalikes-do-they-look-like-they-should>. See also Maximillian Schrems, *Mag. Maximillian Schrems v. Facebook Ireland Limited*, Handelsgericht Wien, 31 July 2014, p. 26-27, accessible at [http://www.europe-v-facebook.org/sk/sk\\_en.pdf](http://www.europe-v-facebook.org/sk/sk_en.pdf) (last accessed 24 August 2015).

<sup>187</sup> Facebook for business, “How do I target ads using my Custom Audiences and/or Lookalike Audiences?”, <https://www.facebook.com/business/help/572787736078838> (last accessed 24 August 2015).

<sup>188</sup> Facebook, “Can I use targeting to narrow down my Custom or Lookalike Audience?” <https://www.facebook.com/help/365659450209683> (last accessed 24 August 2015). Advertisers can only exclude Custom or Lookalike Audiences from their ad campaign. If they wish to additionally exclude on the basis of Facebook’s additional targeting options, they must work with a Facebook marketing partner. Facebook for business, “How do I target ads using my Custom Audiences and/or Lookalike Audiences?”, <https://www.facebook.com/business/help/572787736078838> (last accessed 24 August 2015).



## C. Atlas

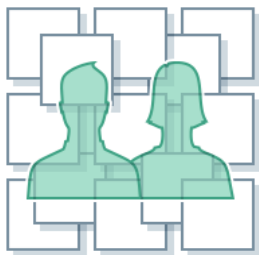
Atlas is an ad serving, management and measurement platform acquired by Facebook in 2013.<sup>189</sup> One of the main reasons for acquiring Atlas was to allow marketers to obtain a more “holistic” view of their ad campaigns **across devices**:

*“[Atlas] will help advertisers close the loop and compare their Facebook campaigns to the rest of their ad spend across the web on desktop and mobile.*

*Our belief is that measuring various touch points in the marketing funnel will help advertisers to see a more complete view of the effectiveness of their campaigns. Acquiring Atlas will be an important step towards achieving this goal.”<sup>190</sup>*

Since its acquisition by Facebook, the Atlas platform has been further developed to support “**people-based marketing**”.<sup>191</sup> People-based marketing is heralded by Atlas as being more accurate than existing targeting mechanisms (which are based primarily on cookies) and for its enhanced ability to target and track people across devices:

*“Atlas delivers people-based marketing, helping marketers reach real people across devices, platforms and publishers. By doing this, marketers can easily solve the cross-device problem through targeting, serving and measuring across devices. And, Atlas can now connect online campaigns to actual offline sales, ultimately proving the real impact that digital campaigns have in driving incremental reach and new sales.”<sup>192</sup>*



### People-Based Marketing

Reach the right people at the right time — where they are.



### Cross-Device

Understand the real actions audiences take, even as they move between devices.



### Online to Offline

See the relationship between online campaigns and in-store conversions with new clarity.



### Prove Real Results

Illuminate and understand customer journeys with more accuracy and impact than ever before.

<sup>189</sup> B. Boland, “Facebook to Acquire Atlas from Microsoft” *Facebook Newsroom*, 28 February 2013, <http://newsroom.fb.com/news/2013/02/facebook-to-acquire-atlas-from-microsoft> (last accessed 24 August 2015)

<sup>190</sup> *Id.*

<sup>191</sup> E. Johnson, “Meet the new Atlas”, *Atlas Blog*, 29 September 2014, <http://atlassolutions.com/2014/09/29/meet-the-new-atlas> (last accessed 24 August 2015).

<sup>192</sup> *Id.*

Atlas **leverages Facebook’s user base** in order to support people-based marketing. In a 2015 Atlas White Paper, the technical process that enables people-based marketing is described as follows:

*“As part of Facebook, [...] Atlas can use a massive “panel” of users from Facebook to enable higher-fidelity, people-based measurement.*

*When a user logs into Facebook for the first time, Facebook syncs the Atlas and Facebook cookies. What exactly is a cookie sync? Facebook writes a version of the user’s Facebook ID into the Atlas cookie, in a way that does not transmit any personally identifiable information. Looking inside an Atlas cookie, one would see a long, meaningless number that is different in every Atlas cookie. However, Atlas can record this number for each subsequent impression, click or conversion event to understand a person’s ad exposures and conversions.”<sup>193</sup>*

In order to support cross-device targeting, Atlas also **links individuals with devices**. Which information is used precisely in order to create such links is unclear, but Atlas’ privacy statement is clear about its aim to associate browsers and devices with individuals:

*“We use all of the information we have to improve, support, and provide our advertising, measurement and reporting Services. To do so more effectively, we may use the information we have to associate the browsers and devices you use so we can provide better and more consistent experiences across browsers and devices and improve our Services.”<sup>194</sup>*

In order to **connect online advertising with offline purchase behaviour**, Atlas uses an approach similar to Facebook’s “Custom Audience” based on Customer lists<sup>195</sup>:

*“Another benefit of people-based measurement is the ability to connect online advertising with real-world events. Imagine, you are a hotel chain that has online booking but also has a 1-800 number for booking. Your marketing to people online, but many of them choose to convert over the phone. It’s hard to gain much insight into those phone conversions, because they don’t have a digital trail. People-based measurement solves this. Similar to Facebook’s “Custom Audiences” targeting product, marketers use Facebook’s massive user base to onboard email addresses of offline converters. Atlas does not see Personally Identifying Information of converters, and the resulting data are for use by Atlas only, not by Facebook.”<sup>196</sup>*

---

<sup>193</sup> Atlas, “The Case for People-based Measurement & Delivery”, p. 4, <https://atlassolutionstwo.files.wordpress.com/2014/12/the-case-for-people-based-measurement-final-1-15.pdf> (last accessed 24 August 2015).

<sup>194</sup> Atlas, “Privacy Policy”, 13 April 2015, <http://atlassolutions.com/privacy-policy> (last accessed 24 August 2015).

<sup>195</sup> Compare *supra*; Section 5.A.1.

<sup>196</sup> Atlas, “The Case for People-based Measurement & Delivery”, p. 7, <https://atlassolutionstwo.files.wordpress.com/2014/12/the-case-for-people-based-measurement-final-1-15.pdf> (last accessed 24 August 2015).

It is worth noting that **Atlas uses information about Facebook users** in order to target and measure ads.<sup>197</sup> Finally, it is important to note that Atlas not only **extends** its people-based marketing **beyond Facebook**<sup>198</sup>, but also brings together the tracking and targeting potential of Facebook's other companies:

*"For example, Instagram – as a publisher – is now enabled with Atlas to both measure and verify ad impressions. And for Atlas advertisers who are already running campaigns through Instagram, Instagram ads will be included in Atlas reporting."*<sup>199</sup>

#### D. Assessment

The previous sections have outlined some of the ways in which Facebook combines and shares personal data about its users. The purpose of this section is not to evaluate these practices as such, but mainly to assess the extent to which they are clearly communicated to Facebook users.

Article 6, b of Directive 95/46/EC requires that personal data must be *"collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"*. The articulation of a specific and legitimate purpose for data collection is a precondition for ensuring the informed consent of users, the legitimacy of processing, and the accountability of data controllers.<sup>200</sup> In cases where personal data are being collected for more than one purpose

*"(...) each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose complies with the law, and to establish what data protection safeguards to apply."*<sup>201</sup>

In our view, Facebook's terms **lack precision and clarity** with regards to how Facebook combines and shares users' personal data. Specifically, Facebook's terms are characterised by (1) use of non-restrictive language; (2) catch-all provisions; and (3) ambiguity as to the actual

---

<sup>197</sup> Rob Sherman, "Explaining Facebook's recent advertising technology updates", 13 April 2015, accessible at <https://www.facebook.com/notes/facebook-and-privacy/explaining-facebooks-recent-advertising-technology-updates/854611164588767> ("Atlas [...] can use information from Facebook – like age and gender – to better serve and measure ads. Facebook de-identifies this information before it is used by Atlas or LiveRail.") (last accessed 24 August 2015).

<sup>198</sup> Atlas, "Why Atlas", <http://atlassolutions.com/why-atlas/introduction> (last accessed 24 August 2015).

<sup>199</sup> E. Johnson, "Meet the new Atlas", *Atlas Blog*, 29 September 2014, <http://atlassolutions.com/2014/09/29/meet-the-new-atlas> (last accessed 24 August 2015)

<sup>200</sup> Article 29 Data Protection Working Party, "Opinion 03/2013 on Purpose Limitation", 2 April 2013, WP 203, p. 15 et seq.

<sup>201</sup> Article 29 Working Party, "Opinion 03/2013 on Purpose Limitation", *l.c.*, p. 16. See also Dutch Data Protection Authority (CBP), "Investigation into the combining of personal data by Google", Report of Definitive Findings, November 2013, p. 60-63, accessible at [https://cbpweb.nl/sites/default/files/downloads/mijn\\_privacy/en\\_rap\\_2013-google-privacypolicy.pdf](https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf).

sources and recipients of data. Moreover, Facebook has failed to put in place adequate user controls in relation to the combination or sharing of personal data.

### 1) Non-restrictive language

Facebook's DUP does not clearly delineate which data is combined and/or shared for which purpose(s). In the section titled "*How do we use this information*", the DUP sets out **four generic purposes** in relation to *all* personal data collected by Facebook, namely:

- (1) "*Provide, improve and develop Services*";
- (2) "*Communicate with you*";
- (3) "*Show and measure ads and services*";
- (4) "*Promote safety and security*".<sup>202</sup>

At such a level of abstraction, it is impossible to determine which data collected by Facebook are being used for which purpose(s).<sup>203</sup> In fact, Facebook literally authorises itself to use *any* of the information it has to achieve *any* of the aforementioned purposes:

*"We use all of the information we have to help us provide and support our Services."*

The following section of the DUP ("*How is this information shared?*") provides further information about Facebook's data sharing practices. The section elaborates upon a number of use cases, but **does not** (or does not systematically) **differentiate** among the data that will be shared for which purposes. In addition, the section contains a provision which is completely **open-ended**, seemingly authorising any form of data sharing across Facebook companies ("*We share information we have about you within the family of companies that are part of Facebook.*").

As regards sharing of data with "*Third-Party Partners and Customers*", the DUP identifies "the types of third parties" with whom Facebook shares information about its users. At first glance, the section gives the impression of clearly specifying the purposes for which specific data are to be shared. Upon closer inspection, however, the section imposes **few actual restrictions**. The section begins by indicating that Facebook will not share "personally identifiable information (PII)" with advertising, measurement and analytics services unless the user provides consent.<sup>204</sup> When and/or how this consent is requested remains unclear, however, nor is there a straightforward way for users to check whether they might have unwittingly consented already to such sharing. More importantly, the next bullet-point still allows for the sharing of *any*

---

<sup>202</sup> See also *supra*; Section 2.B.3.

<sup>203</sup> See also *infra*; Section 10.A.2.

<sup>204</sup> To the extent that shared information is used to target, single out, or otherwise "individuate" specific individuals, it will still constitute processing of "personal data" within the meaning of Directive 95/46. See Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", WP136, 20 June 2007, p. 10-13 and Court of Appeal, *Google Inc. v. Vidal-Hall a.o.*, 27 March 2015, [2015] EWCA Civ 311, paragraph 115, accessible at <http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html>.

information with *any* “vendor, service provider or other partner” who “globally supports [Facebook’s] business”, for a non-exhaustive list of purposes.<sup>205</sup>

## 2) Catch-all provisions

Facebook’s DUP contains a number of “catch-all provisions” which essentially authorise the company to share and/or combine all the data it has access to. Several provisions have already been mentioned above, but it is worth highlighting them again separately:

*“We use all of the information we have to help us provide and support our Services.”*

*“We share information we have about you within the family of companies that are part of Facebook.”*

*“We use all of the information we have about you to show you relevant ads.”*

*“Facebook may share information internally within our family of companies or with third parties for purposes described in this policy.”*

Catch-all provisions such as these – which lack any specificity – significantly **reduce the value of other, more specific provisions** of the DUP and Cookie Policy<sup>206</sup>. After all, the more specific provisions are characterised by the use of hypothetical language (“may”, “can”, or “for example”), thereby indicating they do not provide a comprehensive account. As a result, one inevitably falls back on the catch-all provisions, which set virtually no limits as to what Facebook can do with any of the data it has access to.

## 3) Sources and recipients of data

The use cases described above illustrate that the sharing and combining of data by Facebook can involve different entities. In its policies, Facebook employs **a myriad of terms** to refer to the potential sources and recipients of personal data. The result is confusing, with terms seemingly referring to the same (types of) entities, either with different denominations and/or through the use of umbrella-terms.

---

<sup>205</sup> The DUP merely provides a non-exhaustive list of examples: “*other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys.*”

<sup>206</sup> For example, Facebook’s Cookie Policy alludes to some of the specific ways in which Facebook uses cookies to combine or share data for advertising purposes: “*For example, we use cookies so we, or our affiliates and partners, can serve you ads that may be interesting to you on Facebook Services or other websites and mobile applications. We may also use a cookie to learn whether someone who was served an ad on Facebook Services later makes a purchase on the advertiser’s site or installs the advertised app. Similarly, our partners may use a cookie or another similar technology to determine whether we’ve served an ad and how it performed or provide us with information about how you interact with them. We also may work with an advertiser or its marketing partners to serve you an ad on or off Facebook Services, such as after you’ve visited the advertiser’s site or app, or show you an ad based on the websites you visit or the apps you use – all across the Internet and mobile ecosystem.*”)

The entities which are most prominently featured in the SRR and DUP are the so-called “**Facebook services**”.<sup>207</sup> The SRR defines “Facebook Services” as

*“the features and services we make available, including through  
(a) our website at [www.facebook.com](http://www.facebook.com) and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions);  
(b) our Platform;  
(c) social plugins such as the Like button, the Share button and other similar offerings; and  
(d) other media, brands, products, services, software (such as a toolbar), devices, or networks now existing or later developed.”*

On a separate Help Page (to which the DUP hyperlinks), Facebook provides a different description of “Facebook services”:

*“Facebook offers a wide variety of products and services, including communications and advertising platforms. Many of these products and services — such as the Facebook mobile app, Messenger, and Paper — are part of your Facebook experience. Other services, such as Slingshot, Rooms, or the Internet.org app, offer more independent experiences (ex: they may not require you to register for or sign in to the service using your Facebook account). Certain services, such as Page Manager or Audience Insights, are products that we offer our business partners such as advertisers. All of these Services are covered by our Data Policy, which describes how we collect, use and disclose your information. Sometimes supplemental terms may also apply to specific products or services, which we will tell you about through those services.”*<sup>208</sup>

A second group of entities which are highly privileged by Facebook’s DUP are the “**Facebook companies**”. In the DUP, Facebook grants itself the possibility to share information between these companies, in accordance with their terms and policies.<sup>209</sup> On a separate page, Facebook provides a list of companies owned and operated by Facebook, together with links to their respective privacy policies. The list of companies include a.o. WhatsApp, Atlas, Instagram, Parse and LiveRail.<sup>210</sup> To the average user, it is likely unclear what type of business each company is engaged in, or which data each company might be processing about them. Even if users were to click through to review the information provided for each company, they would quickly find themselves lost when trying to determine what personal data is being processed for which purposes, let alone when and how exactly this happens. Nevertheless, Facebook seemingly

---

<sup>207</sup> The beginning DUP provides that “As you review our policy, keep in mind that it applies to all Facebook brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the “Facebook Services” or “Services.”

<sup>208</sup> Facebook, “What are the Facebook Services?”, <https://www.facebook.com/help/1561485474074139> (last accessed 24 August 2015).

<sup>209</sup> Specifically, the DUP provides that “We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies” and later “We share information we have about you within the family of companies that are part of Facebook”

<sup>210</sup> Facebook, “The Facebook companies”, accessible at <https://www.facebook.com/help/111814505650678> (last accessed 24 August 2014).

expects its users to review the policies of each of these companies in order to understand how their personal data might be used.<sup>211</sup>

In addition to the two aforementioned groups of entities, Facebook's terms also make reference to **many other types of sources and recipients**, i.e.: (1) the Facebook "Platform"<sup>212</sup>; (2) the "family of companies that are part of Facebook"; (3) "applications"<sup>213</sup>; (4) "third-party partners"<sup>214</sup>; (5) "third-party customers"; (6) "third-party companies"; (7) "vendors"; (8) "service providers"; (9) "partners who globally support our business"; (10) "providers of integrated third-party features"<sup>215</sup>; and (11) "advertising, measurement or analytics partners"<sup>216</sup> and (12) "third parties".

#### 4) Inadequate user controls

The combination and sharing of personal data across a wide variety of sources creates additional privacy risks, exceeding those which typically arise in a relationship between a single service provider and its users. Facebook's data collection practices are by no means limited to information which individuals actively and knowingly provide when making use of a Facebook service. In the same vein, the use of collected information by Facebook – or by Facebook's companies – is by no means limited to what individuals might intuitively experience as being part of the Facebook experience.

Because Facebook's combination and sharing of data involves many entities *outside* of Facebook, it constitutes a significant interference in the privacy interests of the individuals concerned.<sup>217</sup> Moreover, such operations are far more likely to go beyond users' reasonable expectations of how their data are being used. Facebook should therefore put in place appropriate user controls

---

<sup>211</sup> Rob Sherman, "Explaining Facebook's recent advertising technology updates", 13 April 2015, accessible at <https://www.facebook.com/notes/facebook-and-privacy/explaining-facebooks-recent-advertising-technology-updates/854611164588767> ("Atlas and LiveRail are Facebook companies that help advertisers and publishers show relevant ads on websites across the internet and in apps on your phone. Today we're updating their privacy policies to reflect recently announced new features of these services [...].")

<sup>212</sup> Article 17(2) of Facebook's SRR defines "Platform" "a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to [Facebook]". In its Platform Policy, Facebook explicitly reserves the right to collect virtually any (personal) data generated/captured by entities on the Platform. See Facebook, Facebook Platform Policy, accessible at <https://developers.facebook.com/policy>. ("We can analyze your app, website, content, and data for any purpose, including commercial. For example, we can analyze your app for targeting the delivery of ads and indexing content for search and measurement.")

<sup>213</sup> Article 17(8) SRR defines "application" as "any application or website that uses or accesses Platform, as well as anything else that receives or has received data from [Facebook]".

<sup>214</sup> The term "third-party partners" is not defined by either the SRR or DUP. It is loosely used to refer inter alia to "advertisers"; "partners Facebook jointly offer services with" and "third party companies who help [Facebook] provide and improve [their] Services or who use advertising or related products".

<sup>215</sup> The cookie policy describes them entities that "integrate third party features like maps or videos to provide [users] with a better service". Cookie Policy: 'The providers of those integrations may collect information when you view or use them, including information about you and your device or browser.'

<sup>216</sup> Mentioned in Facebook's DUP.

<sup>217</sup> See also and J. Rauhofer, "Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?", *European Data Protection Law Review* 2015, Vol. 1, p. 14-15.

to ensure both the legitimacy and fairness of processing. Whereas an opt-out mechanism may be sufficient in some instances where data is combined or shared across “Facebook Services” or “Facebook companies”, other instances will require unambiguous (opt-in) consent.<sup>218</sup> Unambiguous (opt-in) consent is required for any combination and/or sharing of data for advertising purposes. As explained in Chapter 3, however, Facebook only offers an opt-out system for its users to regulate the use of their data regarding their “activities off Facebook” for third-party advertising purpose:

If you don't want Facebook or other participating companies to collect or use information based on your activity on websites, devices, or apps off Facebook for the purpose of showing you ads, you can opt out through the Digital Advertising Alliance in the USA, Digital Advertising Alliance of Canada in Canada or the European Digital Advertising Alliance in Europe. You can also opt out using your mobile device settings.

You only need to opt out once. If you opt out of interest-based advertising from Facebook on one phone or computer, we'll apply that choice everywhere you use Facebook.

As discussed earlier, consent cannot be inferred from the data subject's inaction. As a result, Facebook's current opt-out system for advertising based on activities “off Facebook” does not meet the requirements for legally valid consent.<sup>219</sup>

---

<sup>218</sup> See also CNIL, “Appendix: Google Privacy Policy: Main Findings and Recommendations”, 16 October 2012, p. 7, accessible at [http://www.cnil.fr/fileadmin/documents/en/GOOGLE\\_PRIVACY\\_POLICY-RECOMMENDATIONS-FINAL-EN.pdf](http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-RECOMMENDATIONS-FINAL-EN.pdf).

<sup>219</sup> Cf. supra; Section 2.B.5 and Section 3.D.6.



## 6. Location Data

Smart devices contain many sensors which make it possible to determine the physical location of the person holding it (e.g., GPS, WiFi, etc.).<sup>220</sup> In principle, the Operating System (OS) of a smart device enables its users to decide whether or not to share location data with a particular application. At the level of the OS, users are typically offered a binary choice: allow the app to access location data or not.

One of the permissions requested by the Facebook mobile application (hereafter: “Facebook App”) is access to location data. Users who wish to make use of any of the location-based services within the Facebook App (whether offered by a third party or Facebook itself), must grant the Facebook App full access to the location data of their device. Once the Facebook App is authorised to access location data at OS level, there are no further (in-app) settings to restrict Facebook’s access to location data.

Facebook does offer certain controls with regard to the sharing of location data with other entities. For example, the Facebook App contains a setting entitled “Messenger location services”, according to which users can choose whether or not to share their physical location (by default) with friends through Facebook Messenger. This setting does not, however, prevent Facebook from accessing location data on the device for other purposes.<sup>221</sup> The only way to prevent Facebook from accessing location data on the device is do so at the level of the operating system.<sup>222</sup>

Even when a user decides to turn off Facebook’s access to location data at the OS level, this still does not prevent Facebook from collecting location data via other means.<sup>223</sup> Pictures taken with smartphones, for example, often contain location information as metadata. As a result, location data may be shared indirectly when uploading pictures to Facebook. Combined with features such as facial recognition, it is fairly easy to pinpoint the location of specific individuals to specific locations in time.

On a webpage for advertisers, Facebook states that in order to determine a someone’s location, it “*uses information from multiple sources such as current city from profile, IP address, data from mobile devices if location services are enabled, and aggregated information about the location of*

---

<sup>220</sup> For a more comprehensive analysis see Article 29 Data Protection Working Party, “Opinion 13/2011 on Geolocation services on smart mobile devices”, WP185, 16 May 2011.

<sup>221</sup> With regard to its Messenger App, Facebook has recently stated in a blog post that “*Messenger does not get location information from your device in the background—only each time you select a location and tap Send when you use the Messenger app.*” (S. Chudnovsky, “A New Way to Send a Location in Messenger”, Facebook Newsroom, 4 June 2015, available at <http://newsroom.fb.com/news/2015/06/a-new-way-to-send-a-location-in-messenger> (last accessed 25 August 2015). No such limitation or commitment can be found, however, in Facebook’s 2015 DUP.

<sup>222</sup> See also R. Allan, “Setting the Record Straight on a Belgian Academic Report”, Facebook Newsroom, 8 April 2015, accessible at <http://newsroom.fb.com/news/h/setting-the-record-straight-on-a-belgian-academic-report/> (last accessed 24 August 2015).

<sup>223</sup> For a discussion of how Facebook has increased its access to geo-coded data over time see R. Wilken, “Places Nearby: Facebook as a location-based social media platform”, *New Media & Society* 2014, Vol. 16(7), p. 1087-1103.

friends.”<sup>224</sup> Advertisers can target Facebook users within a particular location in several different ways, with targeting options such as “people recently in this location” and “people traveling in this location”.<sup>225</sup>

#### **A. Facebook’s 2013 DUP**

- “We receive data from or about the computer, mobile phone, or other devices you use [...] This may include network and communication information [...] and other information about things like your [...] location [...]. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby, or we could request device information to improve how our apps work on your device.”
- For example, we [...] may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you in which you might be interested. We may also put together data about you to serve you ads or other content that might be more relevant to you.”
- “When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications.”

#### **B. Facebook’s 2015 DUP**

- “We collect the content and other information you provide when you use our Services, including [...] information in or about the content you provide, such as the location of a photo or the date a file was created.”
- Here are some examples of the device information we collect:  
[...].  
Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.  
Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.  
[...]
- “When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby.”
- “Other people may use our Services to share content about you with the audience they choose. For example, people may share a photo of you, mention or tag you at a location in a post [...].”

---

<sup>224</sup> Facebook, “How does Facebook know when people are in the locations I’m targeting?”, accessible at <https://www.facebook.com/help/133609753380850> (last accessed 25 August 2015).

<sup>225</sup> See Facebook, “What options do I have when selecting people within a location?”, accessible at <https://www.facebook.com/help/755086584528141> (last accessed 25 August 2015).

## C. Assessment

Facebook's 2015 DUP is slightly more explicit about the types of information Facebook collects in order to locate its users (e.g., the 2015 DUP explicitly mentions WiFi signals and Bluetooth as means to determine a user's location). The description of purposes is, however, as vague and broad as it was in 2013 (Facebook still collects the "GPS or other location information" in order to "tailor our Services for you and others"). Interestingly, there is **no longer any mention of limiting the storage or use of location data to the time necessary to provide a service.**

The collection and use of location data by Facebook constitutes processing of personal data.<sup>226</sup> Location data do not qualify as "sensitive data" as defined in article 8 of Directive 95/46. Nevertheless, the Article 29 Working Party has emphasised the particular nature of location data which requires special protection (i.e., opt-in).<sup>227</sup> The special nature of location data is also emphasised in article 9 of the e-Privacy Directive<sup>228</sup>, providing a specific regime regarding information obligations and consent requirements. Providers of OSNs generally do not qualify as providers of an "electronic communication service", meaning Facebook falls largely outside of the scope of the e-Privacy Directive.<sup>229</sup> Nevertheless, a normal reading of article 7 of Directive 95/46 in principle requires informed user consent prior to the sharing of location data.<sup>230</sup>

As result, **Facebook should offer more granular in-app settings for sharing of location data, with all parameters turned off by default.**<sup>231</sup> This should allow users to determine when, how and what (location) data can be collected by Facebook and for what purpose. Additionally, Facebook's DUP should provide more detailed information about **how, when and why exactly** location data is collected. Finally, **location data should only be collected and stored to the extent and for the duration necessary for the provision of a service** explicitly requested by the user.

---

<sup>226</sup> Article 29 Working Party, "Opinion 13/2011 on Geolocation Services on Smart Mobile Devices", WP185, May 16, 2011, p. 9-11 and 13.

<sup>227</sup> *Id.*

<sup>228</sup> Article 9 of the e-Privacy Directive has implemented in Belgian law by way of article 123 of the (revised) Law of 13 June 2005 concerning electronic communication (B.S., 20 June 2006).

<sup>229</sup> See also Article 29 Working Party, Opinion 5/2009 on Online Social Networking, 12 June 2009, p.10.

<sup>230</sup> See also *supra*; Chapter 2 on the role of consent.

<sup>231</sup> Until recently, Facebook's Messenger app would share location information by default with each message, which prompted the creation a Chrome browser extension called the "Marauder's Map", plotting the location of Facebook users on a map over time. See A. Khanna, "Stalking Your Friends with Facebook Messenger — Faith and Future." *Medium*, May 26, 2015. <https://medium.com/@arankhanna/stalking-your-friends-with-facebook-messenger-9da8820bd27d> and H.J. Parkinson, "Marauders Map: The App That Stalks Facebook Messenger Users." *The Guardian*, May 28, 2015. [www.theguardian.com/technology/2015/may/28/marauders-map-chrome-app-tracks-facebook-messenger](http://www.theguardian.com/technology/2015/may/28/marauders-map-chrome-app-tracks-facebook-messenger). See also A. Khanna, "Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger", *Technology Science*, 11 August 2015, accessible at <http://techscience.org/a/2015081101/> (last accessed 20 August 2015).

## 7. Further use of user-generated content

### A. Facebook's IP License

Clause 2 of Facebook's 2015 SRR<sup>232</sup> provides that

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

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

Clause 2 states that **all copyright protected content**, and in particular **photos and videos that users post may be used by Facebook** in either non-commercial or commercial ways. Because the license is non-exclusive, users retain the right to continue to use and exploit their content as well in any way they deem suitable (e.g. grant licences to other parties).

The license is **transferable and sub-licensable**, implying that Facebook may authorise any third party to use protected content of an individual user and receive payment for it. The license is furthermore **royalty-free**, which implies that users will not receive any form of remuneration

---

<sup>232</sup> Clause 2 of Facebook 2013 SRR contained near-identical wording.

nor share in the proceeds that Facebook might collect from third parties in consideration of an authorisation to use photos or videos from users.

The license is **worldwide**, so Facebook may allow use of a user's content on a worldwide basis. In principle, the license is terminated when the protected materials (photos and or/videos) are deleted. However, if the content has been shared with other users who have not deleted it from their profile, the license continues to apply until the date of deletion of a particular content by every user with whom the content has been shared. So basically, the license may be of a perpetual nature in cases where content is shared with others.

**It can be seriously questioned whether such an encompassing type of license is in compliance with copyright law.** As a preliminary matter, it should be observed that the current *acquis communautaire* in the domain of copyright law does not provide an answer to this question as none of the current copyright directives, including the Information Society Directive<sup>233</sup>, include generally applicable provisions in respect of copyright contracting. This issue remains therefore primarily **governed by the national laws of the Member States**. It has been demonstrated that significant differences exist at the national level regarding the law applicable to copyright contracts.<sup>234/235</sup> While in some countries the general principles of contract law continue to apply, some other countries, including Belgium, have included a number of specific safeguards in their copyright legislation with a view to protect authors as the weaker party to transactions relating to the exploitation of their works to prevent that they be unfairly or unreasonably disadvantaged (e.g. over-broad transfers of rights).

**In Belgium**, Article XI.167 BCEL<sup>236</sup> lists the conditions that are applicable to copyright contracts in general.<sup>237</sup> These provisions do not make a distinction between the rules applicable to different types of transfers and, hence, are applicable to assignments as well as (non-exclusive or exclusive) licenses. Firstly, §1 establishes a specific rule of evidence regarding the existence of the license agreement vis-à-vis the author in the sense that any assignee or licensee will need to provide evidence *in writing*. Secondly, copyright contracts are to be interpreted in a *restrictive* manner in favour of the author (*in dubio pro auctore*). Thirdly, with respect to the scope of the rights transferred by the contract, an obligation is imposed to **explicitly address the remuneration, the scope and the duration for each mode of exploitation**. This list should, however, be limited to *known* modes of exploitation provided and the text of the contract should

---

<sup>233</sup> 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, *OJ L167/10*. Changes to this framework are currently being discussed and a proposal for a new legislative instrument is announced for mid 2015.

<sup>234</sup> L. Guibault and P. Bernt Hugenholtz, *Study on the conditions applicable to contracts relating to intellectual property in the European Union*, EU Study contract No. ETD/2000 /B5-3001/E/69, May 2002 (available at <http://www.ivir.nl/publicaties/download/334>).

<sup>235</sup> It should be noted that these existing disparities in the laws of the EU member states relating to copyright contracts will lead to different outcomes depending on which national law applies, e.g. in relation to the initial allocation of rights and further transfer of rights

<sup>236</sup> Belgian Code on Economic Law that codifies, since 1 January 2015, the former provisions of the Belgian Copyright Act (Act of 30 June 1994 on copyright and neighbouring rights).

<sup>237</sup> For more details, see Hendrik Vanhees, 'Artikel 3' in Fabienne Brison and Hendrik Vanhees (Eds.), *De Belgische Auteurswet. Artikelsgewijze commentaar*, Larcier, Brussel 2012, 31.

be sufficiently precise. **Any transfer of rights that would relate to yet *unknown* types of exploitation is null and void.**<sup>238</sup> Moreover, contract clauses by which rights to *future works* are transferred are only valid if they are **restricted to a limited period of time** and provided that the types of works, to which the transfer applies, are specified (§ 2).

Regarding the remuneration, Article XI.167 BCEL does not impose a certain minimum royalty rate. Hence, in principle, a royalty-free license can be validly agreed upon. Finally, any assignee or licensee is obliged to exploit copyright in accordance with honest professional practices as established in the particular sector concerned (§ 1 *in fine*).

It is important to underline that the rules described above are imperative in nature and cannot be contracted away.

It should furthermore be observed that besides economic rights, copyright law also confers *moral rights* on the author, including at least in all European countries the rights of paternity and integrity<sup>239</sup> as well as, at least in the so-called *droit d'auteur* countries, the right of divulgation.<sup>240</sup> These rights are inalienable as a matter of principle.<sup>241</sup> Subject to narrowly defined conditions, it is accepted that a waiver with respect to individual attributes of the moral rights are allowed<sup>242</sup>, but is highly unlikely that the terms of the Facebook license comply with these conditions.

**In Germany**, the question relating to the validity of licensing terms imposed by Facebook was addressed in the case *Verbraucherzentrale Bundesverband*<sup>243</sup>. In its decision of 6 March 2012, the Berlin District Court ruled that, from a copyright perspective, the granting of automatic worldwide exploitation rights by merely clicking on the terms and conditions, was invalid and therefore not enforceable under German Law,

*"(...) The transfer of, as to their nature, unlimited exploitation rights, stipulated in the license, violates the doctrine of intended purpose ("Zweckübertragungslehre") which underlies Article 31, paragraph 5 of the Copyright Act. The doctrine of intended purpose is based on the principle motive of an author having the most extensive share possible in the commercial exploitation of his work and resigning or transferring his exclusive rights to the smallest degree possible. Given its nature as a rule of interpretation, the prerequisite for its application is that there exists doubt concerning the scope of the grant of rights (BGH, 1984, 45, 49 – remuneration clauses in contract on sending). Here - in contrast to the mentioned decision – this is exactly the case, while it is not made explicit in the disputed clause, which*

---

<sup>238</sup> For instance, in the 1980s, forms of exploitation over the Internet did not exist and copyright contracts signed at that time could not validly include these types of exploitation; see case 'Central Station', *Auteurs & Media* 1996/4, 426; confirmed by Court of Appeals of Brussels, 28 October 1997, *Auteurs & Media*, 1997/4, p. 383.

<sup>239</sup> This obligation results from Article 6bis of the Berne Convention.

<sup>240</sup> See, in Belgium, Article 165 § 2 BCEL.

<sup>241</sup> Article XI.165 BCEL

<sup>242</sup> M-Ch. Janssens, "Les droits moraux en Belgique", *Les Cahiers de propriété intellectuelle* (Canada), vol. 25 n° 1, Janvier 2013, p. 91.

<sup>243</sup> Landgericht Berlin, Urteil vom 6. März 2012, (16 O 551/10), accessible at <http://openjur.de/u/269310.html>. An appeal lodged by Facebook was rejected by Kammergericht Berlin, Urteil vom 24. Januar 2014 (5 U 42/12).

*copyright exploitation rights the contracting parties intended to be transferred, rather this clause contains a mere mention of “exploitation of all IP content”. However such a broad transfer contradicts the core idea of the doctrine of intended purpose.”*

The Berlin Court applied Article 31 (5) of the German Copyright Act that specifically deals with contracts in which the scope of the authorised use is not clear and comprehensible. In such a case the scope has to be determined in accordance with the specific purpose of the contract. This principle is known as the “doctrine of intended purpose” and entails that no more rights should be granted than what is needed to achieve the purpose of the transfer. The Berlin Court considered that the broadness of the Facebook’s license terms was in contradiction with the core purpose of transferring copyright under German law and that therefore the provision should be held invalid.

Another question that may arise in relation to the Facebook IP license is whether its provisions can be qualified as “**unfair**” under the **Unfair Contract Terms Directive (UCTD)**<sup>244</sup> (*cf. supra*; section 4 “Unfair Contract terms”). Article 3 of the UCTD deems a contractual term unfair if “*contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer*”.

In order to be applicable, several conditions have to be fulfilled. First, the term must not have been individually negotiated. Article 3 (2) of the Directive explains that a term shall always be regarded as not individually negotiated when “*it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.*” It is up to the seller or the supplier to prove that the term was individually negotiated.<sup>245</sup> Second, there must be a significant imbalance to the detriment of the consumer. Third, that imbalance should be “*contrary to good faith*”.<sup>246</sup> The unfairness shall be assessed on the basis of the nature of the goods or services for which the contract was concluded and by taking into account all the circumstances at the time of concluding the contract.<sup>247</sup> Furthermore, the Annex to the Directive serves as an indication of which kind of terms could be deemed unfair.<sup>248</sup> Until recently, the CJEU has only provided clarifications regarding the unfairness of specific terms, not the general terms used in article 3.<sup>249</sup>

---

<sup>244</sup> Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contract

<sup>245</sup> Unfair Terms Directive, art. 3 (2).

<sup>246</sup> Michael Rustad and Maria Onufrio, ‘Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy’ (2012) 14(4) University of Pennsylvania Journal of Business Law 1085-1190, 1135.

<sup>247</sup> Unfair Terms Directive, art. 4 (1).

<sup>248</sup> H. Schulte-Nölke, C. Twigg-Flesner, M. Ebers (Eds.), *EC Consumer Law Compendium. The Consumer Acquis and its transposition in the Member States*, Sellier. European law publishers, Munich, 2008, p. 228. However, despite a certain level of harmonisation, differences between Member States continue to exist. For instance, some countries have incorporated article 3 (1) literally (e.g. Cyprus, Hungary, Ireland, United Kingdom), others have left out the criterion of ‘good faith’ (Belgium, Greece, Luxemburg).

<sup>249</sup> H.-W. Icklitz, J. Stuyck and E. Terry (eds.), *Cases, Materials and Text on Consumer Law*, (Hart, Oxford/Portland 2010), 289.

However, in a case of March 2013 about mortgage agreements, the CJEU clarified the notions 'significant imbalance' and 'good faith'.<sup>250</sup> According to the CJEU, in order to determine whether a term causes a 'significant imbalance', it must be assessed which rules of national law would apply when there would be no agreement between the parties. This comparative analysis enables the national court to evaluate if the consumer would be worse off under the terms of the agreement than what the national law provides for.<sup>251</sup> As for 'good faith', the CJEU ruled that it must be determined whether the seller, assuming he deals fairly and equitably with the consumer, could reasonably expect that the consumer would have agreed to the term when the contract would have been individually negotiated.<sup>252</sup>

Applying this interpretation of the CJEU on a national level, and taking the Belgian Copyright Act (cf. supra) as an example, it would seem that **Facebook's IP License could be seen to cause a significant imbalance**. As was explained above, a transfer of copyright between the author and the licensor can only be proven by a written agreement. This does not necessarily have to be an individually negotiated agreement; an invoice or a tender from the author can also be regarded as proof that there was a commitment to transfer the copyright.<sup>253</sup> Lacking an agreement in writing, there is no transfer of copyright and any use may give rise to liability for copyright infringement. When considering the obligation of 'good faith', it may be assumed that Facebook users do not intend to give up their intellectual property rights and grant such a broad license to Facebook or, at least, that they would normally not have agreed to such overly broad terms if they would have negotiated an agreement with Facebook on an individual basis. An indication of the latter can be found in the many status updates by which users (re)claim their copyright on content posted on Facebook.<sup>254</sup>

In December 2014, the French Commission for abusive clauses (*Commission des clauses abusives*, CCA), issued a set of recommendations with regard to the terms of use of OSN. According to the

---

<sup>250</sup> Case C-415/11 *Mohamed Aziz v Catalunyacaixa* [2013].

<sup>251</sup> *Ibid*, at paragraph 68.

<sup>252</sup> *Ibid*, at paragraph 69.

<sup>253</sup> H. Vanhees, "Artikel 3", in F. Brison and H. Vanhees (Eds.), *De Belgische Auteurswet. Artikelsgewijze commentaar*, Larcier, Brussel 2012, 32.

<sup>254</sup> "In response to the new Facebook guidelines I hereby declare that my copyright is attached to all of my personal details, illustrations, graphics, comics, paintings, photos and videos, etc. (as a result of the Berner Convention). For commercial use of the above my written consent is needed at all times! (Anyone reading this can copy this text and paste it on their Facebook Wall. This will place them under protection of copyright laws. By the present communiqué, I notify Facebook that it is strictly forbidden to disclose, copy, distribute, disseminate, or take any other action against me on the basis of this profile and/or its contents. The aforementioned prohibited actions also apply to employees, students, agents and/or any staff under Facebook's direction or control. The content of this profile is private and confidential information. The violation of my privacy is punished by law (UCC 1 1-308-308 1-103 and the Rome Statute). Facebook is now an open capital entity. All members are recommended to publish a notice like this, or if you prefer, you may copy and paste this version. If you do not publish a statement at least once, you will be tacitly allowing the use of elements such as your photos as well as the information contained in your profile status updates." (R. Tate, 'Facebook Debunks Copyright Hoax', *Wired* 26 November 2012, accessible at <http://www.wired.com/business/2012/11/facebook-copyright-hoax> .



CCA, IP transfer clauses which are too broad and do not clearly specify “*the content in question, the rights granted and the operations authorized*”, create a significant imbalance.<sup>255</sup>

## B. “Sponsored Stories” and “Social Ads”

Facebook indicates in clause 9 of its 2015 SRR<sup>256</sup> that it can use a user’s profile name, picture and content for commercial purposes as follows:

*“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.”*

In practice, Facebook portrays the content of its users in so-called “Sponsored Stories” and “Social Ads”. A **Social Ad** is similar to a regular advertisement, except that a user’s name and the fact that he or she “liked” a brand are shown next to the ad (an example can be found left from number 3 in the image below). A **Sponsored Story** is a mix between user-generated content and promotional content. A user’s action related to a promotional message is shown with a promotional message in News Feed (this is shown next to number 2). Sponsored Stories should not be mistaken for suggested posts or pages. Those are advertisements that appear in News Feed without any user-generated content attached to it (an example can be found next to number 1).

---

<sup>255</sup> See CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, paragraph 24, accessible at [www.clauses-abusives.fr/recom/index.htm](http://www.clauses-abusives.fr/recom/index.htm) (last accessed 18 March 2015).

<sup>256</sup> Clause 10 of Facebook’s 2013 SRR contained identical wording



According to Facebook,

*“Your profile picture or name may be paired with an ad to show your activity on Facebook (ex: if you follow the Starbucks Page). Keep in mind that your name and profile picture will only appear to the people who have permission to view your Page likes”.*<sup>257</sup>

Sponsored Stories’ and other advertisements (e.g. related posts, suggested posts) are **shown in the News Feed** of a user. The News Feed of a user typically contains status updates and new photos from friends, but also information about new applications, events, etc. For example, a user’s News Feed

*“may include ‘status updates’ from traders whom the user has ‘liked’. They may also include messages indicating that the user’s friends ‘like’ a particular trader, information received because one of the user’s friends has ‘shared’ information about a trader, or messages indicating that a friend has participated in a competition”.*<sup>258</sup>

<sup>257</sup> <https://www.facebook.com/help/214816128640041#Does-Facebook-use-my-name-or-photo-in-ads?>

<sup>258</sup> Nordic Council of Consumer Ombudsmen, “Position of the Nordic Consumer Ombudsmen on social media marketing – Appendix 1: The Consumer Ombudsmen’s interpretation of Directive 2002/58/EC (Directive on Privacy and Electronic Communications) as amended by Directive 2009/136/EC relative to commercial messages on Facebook”, 3 May 2012, p. 1, accessible at <http://www.konsumentverket.se/Global/Konsumentverket.se/Bilaga%201-eng.pdf>

## 1) Unsolicited communications

The question has been raised whether the “Sponsored Stories” of Facebook should be regarded as “unsolicited commercial communications” within the meaning of article 13(1) of the e-Privacy Directive. Article 13(1) provides that

*“[t]he use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.”<sup>259</sup>*

In a letter to Facebook, the **Norwegian Consumer Ombudsman** characterised the News Feed as a “direct marketing” channel which can be compared to e-mails and text messages:

*“The Consumer Ombudsman is of the opinion that advertisements in the News Feed, and especially Sponsored Stories, are quite similar to electronic mail, and that these commercial messages are delivered to consumers through an electronic method of communication that permits individual communication.”<sup>260</sup>*

If Sponsored Stories may indeed be regarded as “unsolicited communications” within the meaning of article 13(1) of Directive, the prior consent from the users concerned is necessary.

The **Nordic Consumer Ombudsmen**, however, were “uncertain” as to whether commercial messages appearing in the News Feed fall within the remit of article 13(1).<sup>261</sup> Given this uncertainty, they argued that such messages should be considered as ‘**other unsolicited communications**’ as defined by Article 13 (3)<sup>262</sup> of the e-privacy Directive and that users must thus be able to opt out of receiving these kind of direct marketing messages.<sup>263</sup>

Facebook currently **offers neither an opt-in nor an opt-out** with respect to receiving Sponsored Stories.

---

<sup>259</sup> Article 13 of the e-Privacy Directive has implemented in Belgian law by way of articles XII.13 and XIV.77 BCEL.

<sup>260</sup> Forbrukerombudet (Consumer Ombudsman Norway), Letter regarding sponsored stories etc. in the News Feed an misleading ads, 11 December 2012, accessible at <http://www.forbrukerombudet.no/2012/12/working-to-stop-spam-and-fake-brand-name-goods-on-facebook>.

<sup>261</sup> Nordic Council of Consumer Ombudsmen, “Position of the Nordic Consumer Ombudsmen on social media marketing – Appendix 1: The Consumer Ombudsmen’s interpretation of Directive 2002/58/EC (Directive on Privacy and Electronic Communications) as amended by Directive 2009/136/EC relative to commercial messages on Facebook”, l.c., p. 1.

<sup>262</sup> “Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.” See art. XIV.78 BCEL.

<sup>263</sup> Nordic Council of Consumer Ombudsmen, “Position of the Nordic Consumer Ombudsmen on social media marketing – Appendix 1: The Consumer Ombudsmen’s interpretation of Directive 2002/58/EC (Directive on Privacy and Electronic Communications) as amended by Directive 2009/136/EC relative to commercial messages on Facebook”, l.c., p. 1.

## 2) Identifying commercial communications

Facebook indicates in clause 9 of its 2015 SRR that users “*understand that we may not always identify paid services and communications as such.*” (cf. supra). According to article 6(a) of the e-Commerce Directive, however, **commercial communication must be clearly identifiable as such.**<sup>264</sup> This issue was also addressed by the Nordic Consumer Ombudsmen:

*“All commercial communications need to be designed and presented in a way to make them clearly identifiable as such and must clearly identify on whose behalf they are made.”*<sup>265</sup>

Also, they argue that if a commercial communication is shown in a place that is normally not reserved for advertisements such as a user’s News Feed on Facebook, there are more severe information requirements.<sup>266</sup>

It is highly questionable whether Facebook properly identifies its Sponsored Stories as commercial communications. To illustrate, the following screenshot can offer an example of an actual Sponsored Story:



<sup>264</sup> European Parliament and Council Directive (EC) 2000/31/EC on certain legal aspects of information society services, in particular economic commerce, in the Internal Market [2000] OJ L178/1 (e-Commerce Directive). This provision is implemented in Belgian law through article XII.12 BCEL.

<sup>265</sup> Nordic Council of Consumer Ombudsmen, “Position of the Nordic Consumer Ombudsmen on social media marketing of 3 May 2012”, p. 4, accessible at <http://www.konsumentverket.se/global/konsumentverket.se/st%C3%A5ndpunkt%20version-eng.pdf>

<sup>266</sup> *Id.* The need to clearly identify and distinguish commercial content from other content is further reinforced by the Directive on unfair commercial practices, which considers as misleading “using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer (advertorial).” <sup>266</sup> European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’), OJ 1.06.2005, L 149.

In the example, User X who liked Fab Europe is only aware of the following story, 'You liked Fab Europe', because this is the message that appears on user X's Timeline. The story is shown differently to his or her Facebook friends. The latter see 'User X liked Fab Europe', followed by a greyed out part that says "related post". This is then followed by promotional content. The greyed out text at the bottom right ("Sponsored") is the only indication that this message is commercial content. As a result, scrolling users are likely to see this Sponsored Story as user-generated content produced by User X. This is deceptive. What is more, the commercial content is shown more prominently than User X's action. Furthermore, in case of a Sponsored Story User X's action will show up more often and to a bigger audience than in case of an "unsponsored" version of the same story.<sup>267</sup> Lastly, the intended message of User X may also be changed or made invisible. In the example below, it seems someone endorsed the ad for a dubious fitness program. While in fact, this person is criticising the advert, which implies he is not endorsing it at all.



---

<sup>267</sup> For example, if User X "likes" an unsponsored item and he shares it with an audience of 100, only 13 will have seen this. If the same item is sponsored, this may increase with more than 100%. Users are unable to control the possible reach of their message because they are unaware of the increase made by Sponsored stories.

### 3) Right to control the use of one's image

Individuals have the right control use of their image. As noted by the European Court of Human Rights:

*“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. Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual’s right to object to the recording, conservation and reproduction of the image by another person.”<sup>268</sup>*

In principle, anyone seeking to record or use the image of another person must first obtain that person’s consent.<sup>269</sup> In legal terms, the right to control one’s image is sometimes also referred to as the “right of personal portrayal” or “portrait right”.<sup>270</sup> The term “portrait” should be understood broadly, as any reproduction of the image or likeness of a person, regardless of the technique or carrier used.<sup>271</sup> The only requirement to invoke the right of personal portrayal is that the individual is sufficiently identifiable, i.e. can be recognised by others.<sup>272</sup>

On an international level, the right to control one’s image is protected by several human rights instruments, such as the European Convention of Human Rights (article 8) and the International Covenant of Civil and Political Rights (article 16).<sup>273</sup> In Belgium, the right of personal portrayal was originally developed through case law. A violation of the right of personal portrayal gives rise to extra-contractual liability (article 1382 of the Belgian Civil Code), but several courts have also recognised an autonomous liability ground in article 10 of the Belgian Copyright Act (now article Art. XI.174 BCEL).<sup>274</sup> In addition, where the use of one’s image constitutes the processing of personal data, the recording and use must comply with the provisions of the Belgian data protection act, which means that the use of one’s image for commercial purposes will require the

---

<sup>268</sup> European Court of Human Rights, *Reklos and Davourlis v. Greece*, 11 December 2008, at paragraph 40.

<sup>269</sup> D. Voorhoof and P. Valcke, *Handboek Mediarecht*, Larcier, 4<sup>e</sup> editie, 2014 p. 239-240.

<sup>270</sup> The right of personal portrayal belongs to the category of ‘personality’ rights protecting the physical, psychological and moral characteristics of a person as well as the related external expression See E. Guldix and A. Wylleman, “De positie en handhaving van persoonlijkheidsrechten in het Belgische privaatrecht”, *T.P.R.* 1999, 1594.

<sup>271</sup> Based on P. De Hert and R. Saelens, “Recht op afbeelding”, *TPR* 2009, afl. 2, 867. The “likeness” of a person includes all external characteristics or the behaviour of a person, such as a special way of dressing, the general attitude of a person, his posture or even a memory of his habits. See also L. Dierickx, “Recht op afbeelding” in X., *Reeks ‘Instituut voor Familierecht en Jeugdrecht KU Leuven*, nr. 89, Antwerpen, Intersentia, 2005, 62.

<sup>272</sup> See e.g. Court of Appeal of Antwerp, 26 March 2007, *Nieuw Juridisch Weekblad* 2007, afl. 170, 801, Voorz. Rb. Brussel 22 oktober 2009, AM 2010, afl. 3, 301. See also D. Voorhoof, “Facebook en de Raad voor de Journalistiek”, *Nieuw Juridisch Weekblad* 2011, afl. 235, p. 39.

<sup>273</sup> See P. De Hert and R. Saelens, “Recht op afbeelding”, *TPR* 2009, afl. 2, 869.

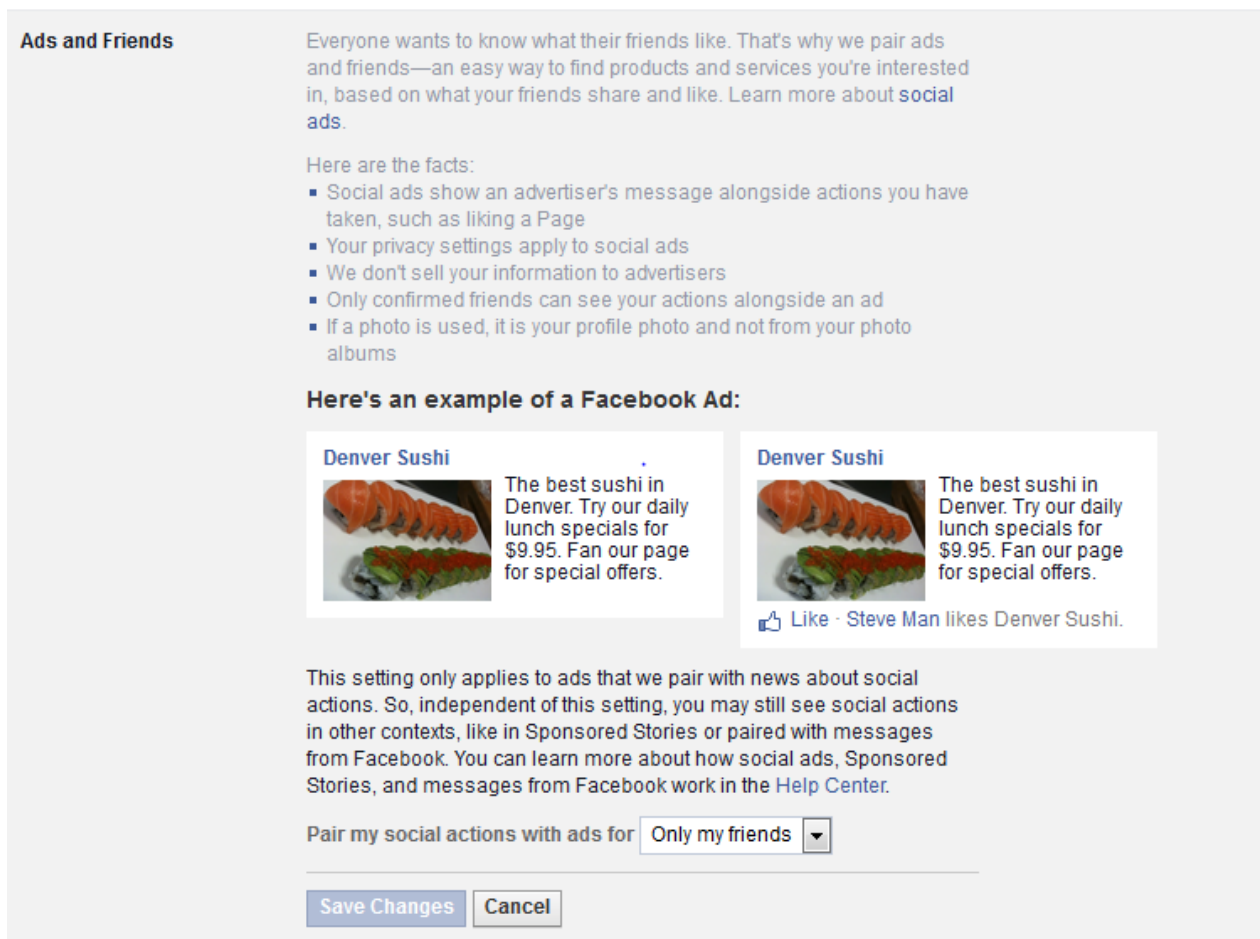
<sup>274</sup> *Id.* For more information see also B. Van Alsenoy and V. Verdoodt, “Liability and accountability of actors in social networking sites”, *SPION* D6.3, December 2014, p. 7 et seq., accessible at [www.spion.me](http://www.spion.me).

unambiguous, free, specific, informed consent of the individual concerned (cf. *supra*; Section 2 “Consent”).<sup>275</sup>

In our view, clause 9 of Facebook’s SRR **does not lead to the unambiguous, free, specific and informed consent** of the individuals concerned. The clause stipulates that

*“If you have selected a specific audience for your content or information, we will respect your choice when we use it.”*

The privacy settings of a user’s account enable the individual to exercise certain controls, as shown in the following screenshot:



<sup>275</sup> See also Commissie voor de Bescherming van De Persoonlijke Levenssfeer, *Aanbeveling nr. 02/2007 van 28 november 2007 inzake de verspreiding van beeldmateriaal*, p. 7, accessible at [http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling\\_02\\_2007\\_0.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_02_2007_0.pdf). In the context of the right to image, Belgian doctrine and jurisprudence generally argue that consent must be explicit, prior, and subject to restrictive interpretation. See D. Voorhoof, ‘Commercieel portretrecht in België’ [2009] [http://www.psw.ugent.be/Cms\\_global/uploads/publicaties/dv/05recente\\_publicaties/VOORHOOF.finalversion.1\\_4.05.2009.pdf](http://www.psw.ugent.be/Cms_global/uploads/publicaties/dv/05recente_publicaties/VOORHOOF.finalversion.1_4.05.2009.pdf)

The default setting for the ad feature is “only my friends”. In other words, the default setting is to allow Facebook to use a person’s profile picture in advertising. So in fact, **an ‘opt-out’ system is used**: the user allegedly “agrees” that Facebook uses his picture for commercial purposes, unless he explicitly changes the privacy settings related to “Ads & Friends”. It can be argued that such “consent” is insufficiently unambiguous and specific to legitimate such processing. Instead, individuals should be asked to consent freely and separately to the use of one’s image for commercial purposes, meaning that **the default setting should be “no one”**.

Furthermore, Facebook states that:

*“This settings only applies to ads that we pair with news about social actions. So, independently of this setting, you may still see social actions in other contexts, like Sponsored Stories or paired with messages from Facebook”.*

In other words, the user is given **no control** as to whether or not his or her profile picture might be used for **Sponsored Stories or other Facebook messages**. The only way to prevent a Sponsored Story is by simply stopping to “like” any page and refrain from any other type of “social action” (which is not clearly defined in any way). Instead, individuals should also be given the ability to control the use of their personal image for the purpose of Sponsored Stories (for which the default setting should also be “no one”).

Finally, we note that there is a significant **lack of transparency** regarding the use of social ads. Users are left in the dark about their appearance in promotional content. For example, it is currently impossible to see one’s own Sponsored Stories. Facebook should not only provide users with more options to control how their data is gathered, but also **show users how their name and picture is used in specific instances**.



## 8. Tracking through social plug-ins

Social plug-ins are website components designed to facilitate the sharing of third-party content within Online Social Networks (OSNs).<sup>276</sup> Examples include: Facebook’s “Like button”, Google+’s “+1” and LinkedIn’s “in share”. While social plug-ins offer benefits to both individuals and website operators, they also make it possible for OSN providers to track users outside the OSN context.<sup>277</sup> For the purposes of this report, we define “**tracking**” as the collection of information about users’ web browsing activities across different websites.<sup>278</sup>

The following section provides a brief introduction on how Facebook tracks individuals through social plug-ins. A more comprehensive technical report is provided in Annex 1.<sup>279</sup>

### A. Tracking of users and non-users

Facebook places cookies whenever someone visits a webpage belonging to the facebook.com domain, even if the visitor is not a Facebook user.<sup>280</sup> For non-users, one of the cookies placed by Facebook (called “datr”) contains a unique identifier and has an expiration date of two years. For users, Facebook uses a range of additional cookies which uniquely identify the user. Once these cookies have been set, Facebook will in principle receive the cookies during every subsequent visit to a website containing a Facebook social plug-in.<sup>281</sup> Facebook will also receive

---

<sup>276</sup> G. Kontaxis, M. Polychronakis, A.D. Keromytis and E.P. Markatos, ‘Privacy-Preserving Social Plugins’, *Proceedings of the 21st USENIX conference on Security symposium*, 2012, p. 30, available at <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final150.pdf>.

<sup>277</sup> *Id.* See also A.P.C. Roosendaal, “We Are All Connected to Facebook ... by Facebook!”, in S. Gutwirth et al. (eds), *European Data Protection: In Good Health?*, Springer, 2012, p. 3-19. An earlier version of this paper is available on SSRN as A. Roosendaal, ‘Facebook tracks and traces everyone: Like this!’, *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2011, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1717563](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563)

<sup>278</sup> Based on F. Roesner, T. Kohno, and D. Wetherall, “Detecting and Defending Against Third-Party Tracking on the Web”, *9th USENIX Symposium on Networked Systems Design and Implementation* (NSDI 2012), accessible at <http://www.franzroesner.com/pdf/webtracking-NSDI2012.pdf> and J.R. Mayer and J.C. Mitchell, “Third-Party Web Tracking: Policy and Technology”, *IEEE Symposium on Security and Privacy*, 2012, p. 1 accessible at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427> (last accessed 21 March 2015). The type of tracking facilitated through social plug-ins is commonly referred as “third party tracking”, due to the fact that the tracker is a different party from the website visited by the user, as displayed in the browser address bar.

<sup>279</sup> Annex 1: G. Acar, B. Van Alsenoy, F. Piessens, C. Diaz and B. Preneel: “Facebook Tracking through social plug-ins”, version 1.0, 25 March 2015, accessible at [https://securehomes.esat.kuleuven.be/~gacar/fb\\_tracking/fb\\_plugins.pdf](https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf) (hereafter: “Annex 1”).

<sup>280</sup> The setting of cookies is not limited to the Facebook homepage, but in principle occurs any time a browser visits any page belonging to the facebook.com domain (provided it has not already been set). For example, a visit to Facebook’s Data Use Policy will result in storage of the datr cookie. The same applies for event pages, company pages, etc. See section 4.1 of Annex 1.

<sup>281</sup> The exact types of cookies and other information collected by Facebook varies depending on whether the person is (i) a logged-in Facebook user, (ii) a logged-out Facebook user, (iii) not a Facebook user and never visited Facebook.com and (iv) not a Facebook user and visited Facebook.com within the last two years but not cleared their cookies in the meantime. (Data Protection Commissioner, ‘Facebook Ireland Ltd. - Report of Audit’, 21 December 2011, p. 81, available at <http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf>, last accessed 22 March 2015). See also sections 4 and 5 of Annex 1.

additional information, including the URL of the webpage visited as well as information about the browser and operating system. This means that:

- Facebook tracks its users across websites even if they do not make use of social plug-ins, and even if they are not logged in; and
- Facebook tracking is not limited to Facebook users.<sup>282</sup>

Facebook's "Like Button", the most popular Facebook social plug-in, is currently present on more than 13 million sites<sup>283</sup>, covering almost all website categories including health and government websites.<sup>284</sup>

## B. Facebook Audits 2011-2012

### 1) The 2011 Report of Audit

In 2011, the Irish Data Protection Commissioner (DPC) investigated social plugins as part of its general audit of Facebook practices. It **concluded that Facebook's collection of data** through social plug-ins **was generally not problematic** as long as Facebook retained only the minimum information necessary for a limited period of time, and **did not use the data for profiling purposes or otherwise associate social plug-in browsing data with users.**<sup>285</sup> At the time, Facebook Ireland ("FB-I") committed itself to

*"amending its data retention policy for social plugin impression logs to provide enhanced protection to the information of users and non-users. Specifically, under its revised policy, for people who are not Facebook users or who are Facebook users in a logged out state, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com. In addition, for all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin."<sup>286</sup>*

In relation to the so-called "**datr**" **cookie**, the Irish DPC noted that:

*"The Datr cookie identifies the web browser used to connect to Facebook. This cookie is used for security, among other purposes. For example, this cookie is also used to underpin login notifications and approvals.*

---

<sup>282</sup> Even if an individual does not have an account with Facebook, the presence of its social plug-ins allows Facebook to keep track of its visits to other pages in which the plug-in has been embedded. (See also A. Roosendaal, 'Facebook tracks and traces everyone: Like this!', l.c., p. 4-8.) For more details see also *infra*; section E.)

<sup>283</sup> <http://trends.builtwith.com/widgets/Facebook-Like> (last accessed 21 March 2015).

<sup>284</sup> A. Chaabane, M.A. Kaafar and R. Boreli, "Big friend is watching you: analyzing online social networks tracking capabilities", *Proceedings of the 2012 ACM Workshop on online social networks (WOSN)*, 2012, accessible at <http://conferences.sigcomm.org/sigcomm/2012/paper/wosn/p7.pdf> (last accessed 21 March 2015).

<sup>285</sup> Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', 21 December 2011, l.c., p. 81-86.

<sup>286</sup> *Ibid*, p. 85.

*The lifetime of this cookie is currently two years. We expect Facebook to examine shortening this period. However, for the reasons outlined in the Security Section we are not raising any concern over the use of this cookie. Our focus is on the use of the data collected and the need to implement a very short retention period where the data collected is from social plug-ins on external websites”<sup>287</sup>*

## 2) The 2012 Report of Re-Audit

The Irish DPC essentially echoed its 2011 position in the 2012 re-audit.<sup>288</sup> It made one exception, however, in relation to a **new cookie** (termed “fr”), which “*FB-I is using in order to monitor browsing by users and not for a security purpose*”.<sup>289</sup> The technical report accompanying the re-audit explains that the fr cookie consists of a **combination of a users’ browser ID and an encrypted version of the logged in users’ Facebook ID**.<sup>290</sup> When asked, Facebook informed the technical auditor that the fr cookie “*is being used by Facebook to deliver a series of new advertisement products*”.<sup>291</sup> In response, the Irish DPC noted that:

*“It is also clear from public statements made by Facebook and indeed the content of the Update Report that the need to generate revenue from advertising will continue to be a key driver for Facebook and that the innovation that it considers necessary in this space will in many instances be underpinned by cookie usage which will require detailed analysis in terms of its compliance with data protection law”<sup>292</sup>*

Facebook was asked by the Irish DPC to provide more detailed information on the use of the fr cookie and the consent collected for this cookie within four weeks.<sup>293</sup> In its annual report for 2012, the Irish DPC indicated that Facebook had satisfied the request for information.<sup>294</sup> To the best of our knowledge, no further details have been made publicly available with regard to the use of the fr cookie as such.

---

<sup>287</sup> *Ibid*, p. 82

<sup>288</sup> Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, p. 28, [https://dataprotection.ie/documents/press/Facebook Ireland Audit Review Report 21 Sept 2012.pdf](https://dataprotection.ie/documents/press/Facebook%20Ireland%20Audit%20Review%20Report%2021%20Sept%202012.pdf), (last accessed 22 March 2015).

<sup>289</sup> *Ibid*, p. 28.

<sup>290</sup> D. O’Reilly, ‘Report on Facebook Ireland (FB-I) Audit 2-3 May & 10-13 July 2012’, 21 September 2012, p. 33, [https://dataprotection.ie/documents/press/Facebook Ireland Audit Review Report 21 Sept 2012.pdf](https://dataprotection.ie/documents/press/Facebook%20Ireland%20Audit%20Review%20Report%2021%20Sept%202012.pdf), (last accessed 22 March 2015).

<sup>291</sup> *Ibid*, p. 34.

<sup>292</sup> Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, l.c., p. 28.

<sup>293</sup> *Ibid*, p. 7

<sup>294</sup> Data Protection Commissioner, “Twenty-Fourth Annual Report of the Data Protection Commissioner 2012”, May 2013, p. 19, accessible at [https://www.dataprotection.ie/documents/annualreports/Annual\\_Report\\_2012.pdf](https://www.dataprotection.ie/documents/annualreports/Annual_Report_2012.pdf) (last accessed 22 March 2015). See also Facebook Ireland Ltd, “Submission by „Facebook Ireland Ltd“ to the Office of the Irish Data Protection Commissioner – Response to complaint(s) number 2”, accessible at [http://www.europe-v-facebook.org/FINAL - Complaint 2 - Shadow Profiles.pdf](http://www.europe-v-facebook.org/FINAL_-_Complaint_2_-_Shadow_Profiles.pdf) (last accessed 23 March 2015).

### C. Facebook's 2013 DUP

Facebook's 2013 DUP describes the collection of data through social plug-ins as follows

*"We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID."*

The 2013 DUP grants Facebook the permission to keep plug-in information for **90 days**.<sup>295</sup> The 2013 DUP also contains a section regarding "Cookies, Pixels & Similar Technologies", which indicates that **cookies can potentially be put to any of the following uses**: (1) authentication; (2) security and site integrity; (3) advertising; (4) localisation; (5) site features and services; (6) performance and (7) analytics and research.

**In 2014, Facebook confirms** that it will begin using information concerning users' browsing activities **for advertising purposes** by default<sup>296</sup>:

*"Let's say that you're thinking about buying a new TV, and you start researching TVs on the web and in mobile apps. We may show you ads for deals on a TV to help you get the best price or other brands to consider. And because we think you're interested in electronics, we may show you ads for other electronics in the future, like speakers or a game console to go with your new TV."*<sup>297</sup>

The Facebook newsroom page **informs users they can "opt out"** as follows:

*"If you don't want us to use the websites and apps you use to show you more relevant ads, we won't. You can opt out of this type of ad targeting in your web browser using the industry-standard Digital Advertising Alliance opt out, and on your mobile devices using the controls that iOS and Android provide."*<sup>298</sup>

---

<sup>295</sup> The 2013 DUP specifies that "We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name and any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you. Learn more at: <https://www.facebook.com/help/social-plugins>"

<sup>296</sup> Facebook, "Making Ads Better and Giving People More Control Over the Ads They See", *Facebook Newsroom*, June 12, 2014, accessible at <http://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/> (last accessed 21 March 2014). See also V. Blue, "Facebook turns user tracking 'bug' into data mining 'feature' for advertisers", *ZDNet* 17 June 2014, accessible at <http://www.zdnet.com/article/facebook-turns-user-tracking-bug-into-data-mining-feature-for-advertisers>. See also K. Hill, "Facebook Will Use Your Browsing and Apps History For Ads (Despite Saying It Wouldn't 3 Years Ago)", *Forbes* 13 June 2014, accessible at <http://www.forbes.com/sites/kashmirhill/2014/06/13/facebook-web-app-tracking-for-ads> (last accessed 21 March 2014).

<sup>297</sup> Facebook, "Making Ads Better and Giving People More Control Over the Ads They See", *Facebook Newsroom*, June 12, 2014, accessible at <http://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/> (last accessed 21 March 2014).

<sup>298</sup> *Id.*

## D. Facebook's 2015 DUP

Facebook's 2015 DUP describes the collection of data through social plug-ins as follows:

*"Information from websites and apps that use our Services.*

*We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us."*

Under the 2015 DUP, **all data collected by Facebook** can potentially be put **any of the following uses**:

- (1) *"Provide, improve and develop Services"* (including personalisation and location-based services);
- (2) *"Communicate with you"*;
- (3) *"Show and measure ads and services"*;
- (4) *"Promote safety and security"*.

On a separate page, Facebook further elaborates on the collection and use of data collected through social plug-ins:

*"What information does Facebook get when I visit a site with the Like button?"*

*If you're logged into Facebook and visit a website with the Like button, your browser sends us information about your visit. [...] The data we receive includes your user ID, the website you're visiting, the date and time and other browser-related info.*

*If you're logged out or don't have a Facebook account and visit a website with the Like button or another social plugin, your browser sends us a more limited set of info. For example, because you're not logged into Facebook, you'll have fewer cookies than someone who's logged in. Like other sites on the Internet, we receive info about the web page you're visiting, the date and time and other browser-related info. We record this info to help us improve our products.*

*As our Data Policy indicates, we use cookies to show you ads on and off Facebook. **We may also use the info we receive when you visit a site with social plugins to help us show you more interesting and useful ads.**"<sup>299</sup>*

In the 2015 Cookie policy, Facebook indicates that information regarding cookies may potentially be put to any of the following uses: (1) authentication; (2) security and site integrity; (3) advertising; (4) localisation; (5) site features and services; (6) performance and (7) analytics

---

<sup>299</sup> Facebook, "About Social Plugins", <https://www.facebook.com/help/social-plugins> (last accessed 22 March 2015)

and research. The 2015 use classification for cookies corresponds to the 2013 use classification for cookies, pixels & similar technologies. However, the **language corresponding with each use category has been modified**. Another notable difference between the 2013 and 2015 DUP is that **the retention limitation of 90 days for cookies collected through social plug-ins is now absent**. In the “Ads” setting, users are again told they can “**opt out**” in relation to the use of web tracking information for advertising purposes:

*“If you don’t want Facebook or other participating companies to collect or use information based on your activity on websites, devices, or apps off Facebook for the purpose of showing you ads, you can opt out through the Digital Advertising Alliance in the USA, Digital Advertising Alliance of Canada in Canada or the European Digital Advertising Alliance in Europe. You can also opt out using your mobile device settings.*

*You only need to opt out once. If you opt out of interest-based advertising from Facebook on one phone or computer, we’ll apply that choice everywhere you use Facebook.”*

## **E. Assessment**

### **1) Article 5(3) of the e-Privacy Directive**

Pursuant to article 5(3) of the e-Privacy Directive, cookies placed via social plugins require **prior consent** from the individual concerned.<sup>300</sup> Article 5(3) contains two exemptions to the requirement of prior consent, namely

- A) for storage or access carried out for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- B) for storage or access which is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

---

<sup>300</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L-201, 31 July 2002, 37-47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *O.J.* L-337, 18 December 2009. 11-36. Article 5(3) of the e-Privacy Directive has implemented in Belgian law by way of article 129 of the (revised) Law of 13 June 2005 concerning electronic communication (B.S., 20 June 2006).

## 2) Position of the Article 29 Working Party

In 2012, the Article 29 Working Party adopted an Opinion clarifying the meaning of the two exemptions contained in article 5(3).<sup>301</sup> As far as social plug-ins are concerned, the Opinion makes a **two-fold distinction**. First, it makes a distinction between “members” and “non-members”. Second, regarding members, an additional distinction is made depending on whether the member is logged in or not.

As far as **non-members** are concerned, the Opinion states that

*“Since by definition social plug-ins are destined to members of a particular social network, they are not of any use for non members, and therefore do not match CRITERION B for those users.”<sup>302</sup>*

According to the Working Party, the same finding applies in relation to **users** of the social network who are **not logged in**:

*“This can be extended to actual members of a social network who have explicitly “logged-out” of the platform, and as such do not expect to be “connected” to the social network anymore.*

*[...]*

*On the other hand, many “logged in” users expect to be able to use and access social plug-ins on third party websites. In this particular case, the cookie is strictly necessary for a functionality explicitly requested by the user and CRITERION B applies. Such cookies are session cookies: to serve their particular purpose, their lifespan should end when the user “logs-out” of his social network platform or if the browser is closed. Social networks that wish to use cookies for additional purposes (or a longer lifespan) beyond CRITERION B have ample opportunity to inform and gain consent from their members on the social network platform itself.”<sup>303</sup>*

Finally, it is worth noting that the requirement of article 5(3) of the e-Privacy Directive in no way diminishes a controller’s obligations pursuant to Directive 95/46. Where the collection or use of cookies amounts processing of personal data, the controller is obliged to comply with all

---

<sup>301</sup> Article 29 Data Protection Working Party, “Opinion 04/2012 on Cookie Consent Exemption”, WP194, 7 June 2012, accessible at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf).

<sup>302</sup> *Ibid*, p. 9

<sup>303</sup> *Ibid*, p. 9. With respect to “user centric security cookies”, the Working Party also notes that “The exemption that applies to authentication cookies under CRITERION B (as previously described) can be extended to other cookies set for the specific task of increasing the security of the service that has been explicitly requested by the user. This is the case for example for cookies used to detect repeated failed login attempts on a website, or other similar mechanisms designed to protect the login system from abuses (though this may be a weak safeguard in practice). This exemption would not however cover the use of cookies that relate to the security of websites or third party services that have not been explicitly requested by the user.” (*Ibid*, p. 7).

requirements including the principle that no more personal data should be processed than is necessary (article 6(1)c).

### 3) Facebook's tracking of users

Whenever a Facebook user visits a third-party website which contains a social plug-in, Facebook receives several cookies.<sup>304</sup> According to its 2015 cookie policy, Facebook collects and uses cookie information for advertising purpose even if the user is logged out:

*"Do we use cookies if you don't have an account or have logged out of your account?"*

*We still use cookies if you don't have an account or have logged out of your account. For example, if you have logged out of your account we use cookies to help:*

*[...]*

*Enable us to deliver, select, evaluate, measure and understand the ads we serve on and off Facebook (this includes ads served by or on behalf of our affiliates or partners)"*<sup>305</sup>

In the "Ads" setting, users are told they can "**opt out**" in relation to the collection or use of tracking information for advertising purposes:

*"If you don't want Facebook or other participating companies to collect or use information based on your activity on websites, devices, or apps off Facebook for the purpose of showing you ads, you can opt out [...]"*

In other words: **Facebook tracks its users for advertising purposes across non-Facebook websites by default**, i.e. unless users take steps to opt-out. Even if the user takes the additional step to opt out, he or she will still be tracked by Facebook<sup>306</sup>, but Facebook *promises* it won't use the information for ad targeting purposes.

If a Facebook user does not opt-out, Facebook takes the inaction to mean that the user wishes to be tracked across third party websites for ad targeting purposes. The current opt-out mechanism has been criticised extensively. First, it has been argued that certain language used by Facebook

---

<sup>304</sup> If the user is logged in to Facebook, Facebook receives a total of 11 cookies. The cookies include a Facebook ID cookie (c\_user), a browser ID cookie (datr) and an encrypted Facebook ID and browser ID cookie (fr). If a user is logged out, Facebook still collects a total of four cookies, including the browser ID cookie (datr) and the encrypted Facebook ID and browser ID cookie (fr). See section 5 of Annex 1.

<sup>305</sup> See <https://www.facebook.com/help/cookies> (last accessed 22 March 2015)

<sup>306</sup> Facebook still tracks logged out users through datr and fr cookie, which contain a user's browser ID and a combination of encrypted Facebook ID and browser ID, respectively. The main difference between logged-in and logged-out users is that logged-out users are not tracked by means of the c\_user cookie (which contains the Facebook ID). Still, the collection of the fr and datr cookies is enough to identify individual Facebook users when they visit websites containing social plug-ins. See section 5.2 of Annex 1.



is misleading and could easily be misunderstood by users (see e.g. TACD<sup>307</sup> and EDRI<sup>308</sup>). The second criticism is that opt-out mechanisms place the onus entirely with users. As emphasised by the Article 29 Working Party, an opt-out mechanism “*is not an adequate mechanism to obtain average users informed consent*”, particularly with regard to behavioural advertising.<sup>309</sup> This means that **Facebook’s current opt-out approach does not satisfy the requirements for legally valid consent.**<sup>310</sup> Moreover, our findings indicate that Facebook still tracks users who are logged out and have opted out from advertising using the opt-out sites recommended by Facebook.<sup>311</sup>

#### 4) Facebook’s tracking of non-users

Facebook also tracks non-users through its social plug-ins, as documented in section 4 of Annex 1. In the past, Facebook would typically only begin tracking non-users after they visited a page belonging to the facebook.com domain. Recent findings indicate, however, that Facebook sometimes also tracks non-users even if they managed to stay clear from the facebook.com domain entirely.<sup>312</sup>

It is important to note that tracking of non-users initiates even if one does not visit the Facebook homepage. In principle, any page belonging to the facebook.com domain will result in the placement of a long-term, identifying cookie (e.g., an event page, a shop page, fan page, ...). It is

---

<sup>307</sup> In an open letter, consumer and privacy advocates expressed their concern to both the FTC Irish Data Protection Commissioner in relation to Facebook’s 2014 announcement that it will begin using information regarding user’s browsing activities for advertisement purposes. See Trans Atlantic Consumer Dialogue, Letter from BEUC and CDD to Chairwoman E. Ramirez and B. Hawkes, 29 July 2014, accessible at <http://tacd.org/wp-content/uploads/2014/07/TACDletter-to-FTC-and-Irish-Data-Protection-Commissioner-re-Facebook-data-collection.pdf> (“Facebook has now completely reversed its stance to the detriment of users of the service. Contrary to its prior representations, upon which users may have relied, the company will now routinely monitor the web browsing activities of its users and exploit that information for advertising purposes.”) The letter also states that Facebook has “misrepresented the amount of control users will be able to exert over their privacy settings. Facebook has stated that it will collect user data from third-party sites, but users will be able to “control which ads” they see. This is misleading; the new data collection policy is unrelated to users’ control over Facebook’s ability to collect browsing information. In fact, the extent to which users can “control the privacy of any covered information maintained by” Facebook is determined by their third-party opt-out cookie”. (Ibid, p. 2-3)

<sup>308</sup> J. MacNamee, “Facing a challenge – understanding Facebook’s opt-out instructions”, EDRI, 11 February 2014, <https://edri.org/facing-challenge-understanding-facebooks-opt-out-instructions/>

<sup>309</sup> Article 29 Working Party Opinion 2/2010 on online behavioural advertising, *l.c.*, p. 15.

<sup>310</sup> See also Article 29 Data Protection Working Party, “Letter from the Article 29 Working Party addressed to Online Behavioural Advertising (OBA) Industry regarding the self-regulatory Framework”, 23 August 2011, accessible at [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803\\_letter\\_to\\_oba\\_annexes.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf). See also Article 29 Working Party, “Working Document 02/2013 providing guidance on obtaining consent for Cookies”, WP 208, 2 October 2013, p. 4. See also supra; section 1 “Consent”

<sup>311</sup> In addition to the datr cookie, which contains a browser ID, Facebook will also receive the fr cookies, which contains a combination of browser ID and an encrypted version of Facebook ID, even if the user is logged out. In 2012, Facebook admitted to be using the fr cookie for certain advertising products. See also infra; section 8.E.5).

<sup>312</sup> Our findings indicate that Facebook places the datr cookie as a third party on some non-Facebook websites. Specifically, we observed that Facebook sets a datr cookie on a small number of external websites which include Facebook Connect or social plug-ins which make a request to the pixel.facebook.com domain. Section 4.2 of Annex 1.

also worth noting that non-users who visit a Facebook page are generally not requested to provide their consent prior to placement of cookies, nor are they provided with a clear notice.

Facebook's 2015 cookie policy implies that the setting of cookies on non-users' browsers is necessary for security purposes.<sup>313</sup> The Article 29 Working Party has taken the position that certain "security cookies" may fall under the exemptions of article 5(3), but only if they are strictly necessary to provide a service explicitly *requested by the user*.<sup>314</sup> The exemption does not, however cover the use of cookies for the security of websites or services that have not been explicitly requested by the user.<sup>315</sup> As a result, **Facebook's tracking of non-users**, even if the data is not used for ad targeting or other purposes, **violates article 5(3) of the e-Privacy Directive**.

### 5) Facebook's proposed opt-out mechanism

In March 2015, we studied Facebook's proposed opt out mechanism in order to assess its effects on cookie-based tracking.<sup>316</sup> As indicated above, Facebook refers its users to external websites if they wish to opt out of advertising based on their activities "*on websites, devices, or apps off Facebook*". There are a total of three websites listed: one for European users<sup>317</sup>, one for Canadian users<sup>318</sup> and one for US users<sup>319</sup>.

If a Facebook **user** opts out, Facebook promises to stop collecting or using browsing information *for the purpose of showing ads*. Running a number of tests, we confirmed that Facebook still tracks its users when they visit a webpage containing Facebook social plugins, even after the user "opts out". It is worth noting that one of the cookies collected by Facebook is the "fr cookie", which Facebook admitted to be using for certain advertising products in 2012.<sup>320</sup>

We then analysed the effect of "opting out" for **non-users** of Facebook, who have not yet received any cookie from Facebook. Testing the European opt-out website, we found that Facebook sets a long term identifying cookie ("datr") during the opt-out process.<sup>321</sup> All subsequent visits to pages including Facebook social plug-ins can be tracked and linked by Facebook using this cookie

---

<sup>313</sup> Specifically, the 2015 Cookie policy provides that Facebook states that "*We also set cookies if you don't have a Facebook account, but have visited facebook.com, to help us protect Facebook Services and the people who use it from malicious activity. For example, these cookies help us detect and prevent denial-of-service attacks and the mass creation of fake accounts. If you have cookies on your browser or device, we read that cookie when you visit a site with a social plugin.*"

<sup>314</sup> Only limited (and dated) information exists as to how precisely Facebook uses data obtain through datr cookie or other cookies for "security" purposes, so it is not possible to comment on its "strict necessity" at this stage.

<sup>315</sup> Article 29 Data Protection Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *l.c.*, p. 7

<sup>316</sup> See <https://www.facebook.com/about/ads> (last accessed 23 March 2015). See section 6.1.1 of Annex 1.

<sup>317</sup> <http://www.youronlinechoices.eu>

<sup>318</sup> <http://youradchoices.ca/>

<sup>319</sup> <http://www.aboutads.info/choices/>

<sup>320</sup> Cf. *supra*; section 8.B.2)

<sup>321</sup> Facebook sets four cookies during the status check on the EDAA opt-out site. The long term identifying cookie placed by Facebook is the so-called "datr" cookie, which is placed in addition to the opt-out cookie ("oo"). If the non-user already visited a page belonging to the facebook.com domain, Facebook does not set a new ("datr") cookie during the opt-out process, as Facebook will have already set it previously.

which will by default remain in the non-user's browser for a period of two years. Interestingly, the opt out site still reports "No Cookie Found" from Facebook *after* the cookies have been set. The cookie status was not updated even if we reloaded the page. In other words: for those individuals who are not being tracked by Facebook (e.g. non-users who have never visited a page on the facebook.com domain, or Facebook users who clear their cookies after logging out from Facebook), **using the "opt out" mechanism proposed for the EU actually enables tracking by Facebook.** What is more, we found that **Facebook does not place any long term identifying cookie on the opt-out sites suggested by Facebook to US and Canadian users.**<sup>322</sup>

## 6) Alternatives

It is worth noting that there are **several tools** that make it possible for website operators to limit Facebook's tracking through plug-ins. The "Social Share Privacy tool", for example, enables website operators to de-activate social plug-ins until a visitor indicates a wish to use them.<sup>323</sup> By default, a grey mock-up image of the social plug-in is shown. Only if a user clicks this image will the "real" plug-in be loaded (and information be sent to Facebook). With a second click, the user can make use of the plug-in.<sup>324</sup> The French Data Protection Authority (CNIL) has in fact endorsed this approach as a means to achieve compliance.<sup>325</sup>

Facebook's responsibilities as data controller, however, exist independently of the responsibilities of website operators. As a result, **Facebook should design its social plug-ins in way which are privacy-friendly by default**, so that website operators are able to provide users with the convenience of social plug-ins, but without unnecessarily exposing data to Facebook.

Until recently (March 2015), Facebook offered developers 4 different types of integrations for Like buttons.<sup>326</sup> In the case of the first 3 integrations, Facebook does by default receive information about the visited website, even if the person does not click the button. If a website operator used the 4th type of integration ("URL") as a link, however, Facebook does **not** receive cookies or other information about the website visit (unless the user actually clicks on the button). In March 2015, Facebook removed the different integration options and only retained one (previously named "HTML5"). The current integration does automatically trigger transmission of cookies as well as the other information highlighted above. To the best of our knowledge, Facebook has not made any statement regarding its decision to remove the three other integration options.

---

<sup>322</sup> <http://www.aboutads.info/choices>; <http://youradchoices.ca>. See section 6.2.2 of Annex 1.

<sup>323</sup> For more information see <http://panzi.github.io/SocialSharePrivacy/>

<sup>324</sup> Id.

<sup>325</sup> See Commission Nationale de l'Informatique et des Libertés (CNIL), Solutions pour les boutons sociaux, <http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/outils-et-codes-sources/les-boutons-sociaux>

<sup>326</sup> The integration types were labelled "HTML5" / "XFBML" / "iFrame" / "URL".

## 9. Fingerprinting

Tracking techniques evolve constantly. While cookies remain the dominant tracking mechanism of the Web, one can also observe an increased usage of “**cookie-less**” tracking techniques.<sup>327</sup> One example is so-called “fingerprinting”, which enables unique identification of a device or application (e.g., a Web browser) without the use of cookies.<sup>328</sup>

Fingerprints are generated by **combining different information elements** relating to a particular device or application instance (e.g., HTTP header information, operating system type and version, screen dimensions, installed plug-in information, etc.).<sup>329</sup> While these information elements do not enable unique identification by themselves, combining them can provide a “fingerprint” which is sufficiently unique to track a device or application instance.<sup>330</sup> The most well-known forms of fingerprinting are “device fingerprinting” and “browser fingerprinting”.

### A. Facebook’s 2013 DUP

Facebook’s 2013 DUP describes the *collection of device information* as follows:

*“We receive data from or about the computer, mobile phone, or other devices you use to install Facebook apps or to access Facebook, including when multiple users log in from the same device. This may include network and communication information, such as your IP address or mobile phone number, and other information about things like your internet service, operating system, location, the type (including identifiers) of the device or browser you use, or the pages you visit.”*

Facebook’s 2013 DUP describes the *use of device information* as follows:

*“For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby, or we could request device information to improve how our apps work on your device.”*

---

<sup>327</sup> See G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan and C. Diaz, “The Web Never Forgets: Persistent Tracking Mechanisms in the Wild”, CCS’14, November 3–7, 2014, Scottsdale, Arizona, USA, accessible at [https://securehomes.esat.kuleuven.be/~gacar/persistent/the\\_web\\_never\\_forgets.pdf](https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf). See also O. Tene and J. Polonetsky, “To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising’, *Minnesota Journal of Law, Science & Technology* 2012, vol. 13, no. 1, p. 288 et seq.

<sup>328</sup> Based on Article 29 Data Protection Working Party, “Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting”, WP224, 25 November 2014.

<sup>329</sup> See Article 29 Data Protection Working Party, “Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting”, *l.c.*, p. 4-5; N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, “Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting”, *IEEE Symposium on Security and Privacy 2013*, p. 2-3, accessible at [http://www.cs.ucsb.edu/~vigna/publications/2013\\_SP\\_cookieless.pdf](http://www.cs.ucsb.edu/~vigna/publications/2013_SP_cookieless.pdf) and O. Tene and J. Polonetsky, “To Track or “Do Not Track”, *l.c.*, p. 295.

<sup>330</sup> Article 29 Data Protection Working Party, “Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting”, *l.c.*, p. 6.

Facebook's 2013 DUP contains a section regarding "Cookies, pixels and other similar technologies".<sup>331</sup> **Device information (or device fingerprinting) is neither mentioned nor alluded to as a technology "similar" to cookies.**

## B. Facebook's 2015 DUP

Facebook's 2015 DUP describes the *collection* of device information as follows:

*"We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices.*

*Here are some examples of the device information we collect:*

*Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.*

*Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.*

*Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address."*

At first glance Facebook's 2015 DUP contains no specific terms on the *use* of device information. However, in the section regarding "Cookies, pixels and other similar technologies", **device information is alluded to as a being "similar" technology**.<sup>332</sup> Moreover, there is a new subsection<sup>333</sup> in the cookie policy which states that

*"We may place or use these technologies when you interact with our Services, our related companies, or with an advertiser or partner (whether or not you are logged in to the particular Service) using a browser or device that permits the placement or use of the relevant technology. For example, when you visit our site or use our app, we may place or read cookies or receive information from your devices. We may also place cookies through a pixel on an advertiser's or partner's site."*

**In addition, all device information now falls under the general use terms** of Facebook's 2015 Cookies policy, meaning that it can potentially be put to any of the following uses: (1) authentication; (2) security and site integrity; (3) advertising; (4) localisation; (5) site features and services; (6) performance and (7) analytics and research.

---

<sup>331</sup> <https://www.facebook.com/about/privacy/cookies>

<sup>332</sup> For example, the 2015 cookie policy, next to "advertising, insights and measurements" provides that "*Things like Cookies and similar technologies (such as information about your device or a pixel on a website) are used to understand and deliver ads, make them more relevant to you, and analyze products and services and the use of those products and services.*"

<sup>333</sup> The title of this subsection is "When might we use cookies, *device identifiers*, local storage or similar technologies?"

## C. Assessment

In 2014, the Article 29 Working Party held that article 5(3) of the e-Privacy Directive also applies to device fingerprinting. Specifically, it reasoned that

*“any processing which [a] third-party undertakes which influences the behaviour of that device or otherwise cause it to store or give access to information on that device, or exposed by that device is within the scope of Article 5(3).”*<sup>334</sup>

This means that any tracking of individuals (users or non-users) through fingerprinting must meet the requirements of article 5(3) of the e-Privacy Directive. **It is highly questionable whether the envisaged collection or use of device information envisaged by the 2015 DUP will comply with the requirements of article 5(3) in practice.** Third-party fingerprinting can intrude upon privacy in the same way as third-party cookies. It can be even more intrusive, as fingerprinting techniques enable trackers to avoid detection more easily and can be more difficult to counter by individuals (e.g., clearing out cookies from one’s browser won’t do the trick).<sup>335</sup>

At this stage, we do not have any technical evidence to suggest Facebook is currently uses fingerprinting for behavioural profiling purposes. The terms of the 2015 DUP are problematic in this respect, however, because they grant Facebook the permission to use any information collected (including device information) for any of the seven use categories identified (including analytics and advertising).

---

<sup>334</sup> Article 29 Working Party, “Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, 25 November 2014, p. 8.

<sup>335</sup> N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna, “Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting”, l.c., p. 2; J.R. Mayer and J.C. Mitchell, “Third-Party Web Tracking: Policy and Technology”, l.c., p. 9.

## 10. Data Subject Rights

Articles 10 and 12-14 of Directive 95/46 grant certain rights to individuals whose data are being processed (“data subjects”). Most relevant to our current analysis are (a) the right to information; (b) the right of access and (c) the rights to object and to erasure.

### A. Right to information

Articles 10 and 11 of Directive 95/46 set out the information obligations of data controllers.<sup>336</sup> As a rule, each data subject must be informed of at least the *identity of the controller* (and, if applicable, of his representative) and the *purposes* of the processing.<sup>337</sup> In addition, Member States may require data controllers to provide the data subject with supplemental information “in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee *fair processing* in respect of the data subject”. Such additional information can refer to the *recipients* or *categories of recipients* of the data, information with regard to the existence of the *right of access, the right to rectify inaccurate data, etc.*<sup>338</sup>

#### 1) Identity of the controller

Facebook’s 2015 DUP identifies its establishment in Ireland (“Facebook Ireland Ltd.”) as the data controller for individuals living outside the US or Canada.

#### 2) Purposes of the processing

Facebook’s 2015 DUP provides a broad overview of the purposes for which it processes personal data. The overview is, however, extremely generic and extends to all data collected by Facebook. Furthermore, Facebook’s current DUP contains virtually no restrictive formulations. Instead, it

---

<sup>336</sup> At the outset, these provisions make a distinction between two scenarios: one in which the information is obtained directly from the data subject (art. 10) and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11). The notice obligations of the controller in each scenario are largely similar; the main differences concern (a) the moment by which notice must be provided and (b) the exemptions to the notice obligation. In situations of indirect collection, for example, the controller is exempted when the “provision of such information proves impossible or would involve a disproportionate effort”. Both provisions have been implemented into Belgium law through article 9 BDPA.

<sup>337</sup> The use of plural “purposes”, in Articles 10-11, implies that the data subject has to be informed not only about the main purpose to be accomplished, but also about any secondary purposes for which the data will be used. See also D. Korff, ‘Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Country Study A.4 – Germany’ (2010), p. 33, available online at [http://ec.europa.eu/justice/policies/privacy/docs/studies/new\\_privacy\\_challenges/final\\_report\\_country\\_report\\_A4\\_germany.pdf](http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf) (last accessed on 23 March 2011), commenting on the relevant provision of the German Data Protection Act, which uses the term “purposes” as well.

<sup>338</sup> Article 9 BDPA provides that controllers must provide such information “*unless it is unnecessary*” to ensure fairness of processing. In other words, the burden of proof lies with the controller to demonstrate why it would be unnecessary to provide information about recipients and/or data subject rights.

primarily contains examples and indications that certain processing operations *might* be possible. As a result, it is extremely difficult (or even impossible) for any individual to ascertain to which uses specific data are actually being put.<sup>339</sup>

The Article 29 Working Party has made clear that indistinct language (*we can/may/...*) and/or hypotheticals (*such as/for example/...*) should be avoided.<sup>340</sup> In Facebook's DUP, the words "*for example*" appear 7 times; "*such as*" 17 times; "*may use/share/receive/...*" 18 times; "*can access/include/share/be seen...*" 4 times. In addition, Facebook's Cookie policy contains the words "*for example*" 18 times; "*such as*" 7 times; and "*may change/interfere/use/store/obtain*" 31 times.

Moreover, information provided regarding the purpose(s) of processing must be sufficiently specific.<sup>341</sup> A purpose that is vague or general (e.g. "improving user experience", "marketing purposes", "IT-security purposes") will - without further detail - generally not meet the criteria of being "specific".<sup>342</sup> While providing an overarching broader purpose might be useful, it does not exempt the controller from the duty to specify each purpose with sufficient detail.<sup>343</sup> The level of detail required with which purpose should be specified depends on context in which data are collected and the type(s) of personal data involved.<sup>344</sup>

### **3) Recipients or categories of recipients**

Facebook's DUP does not clearly identify all the recipients or categories of recipients of personal data. While the concept of "Facebook Services"<sup>345</sup> is defined, other concepts such as "third party companies", "service providers" and "other partners" are not defined at all. As a result, users are unable to determine with whom their data might actually be shared.

### **4) Categories of data**

Facebook's DUP does not provide a single comprehensive overview of the categories of personal data being collected. While Facebook has published, on a separate page, a list entitled "*What*

---

<sup>339</sup> See also *supra*; Section 5.D.

<sup>340</sup> Article 29 Working Party. Letter to Larry Page. "Google Privacy Policy - Appendix" September 23, 2014, p. 2) See also CNIL, "CNIL Review of Google's New Privacy Policy : Incomplete Information and Uncontrolled Combination of Data across Services," October 16, 2012, p. 2 and College Bescherming Persoonsgegevens. *Investigation into the Combining of Personal Data by Google - Report of Definitive Findings*. Den Haag: College Bescherming Persoonsgegevens, November 2013, p. 66-68.

<sup>341</sup> Article 6(1)(b). See also Article 29 Working Party. "Opinion 03/2013 on Purpose Limitation", Brussels, 2 April 2013, p. 15 *et seq.*

<sup>342</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, l.c., p16.

<sup>343</sup> Id.

<sup>344</sup> Id..

<sup>345</sup> The list of Facebook companies includes, *inter alia*, Instagram, WhatsApp, Atlas, Oculus, a.o.. See: <https://www.facebook.com/help/111814505650678>. For more on Facebook's combining of personal data, see Chapter 5 of this report.



*categories of my Facebook data are available to me?*<sup>346</sup> the list also does not encompass the full inventory of personal data being collected by Facebook.<sup>347</sup>

## 5) Data subject rights

Facebook's DUP does not inform data subjects of the existence of their right of access or the right to rectify inaccurate data. In fact, Facebook does not make any explicit mention of any of the data subject rights provided by Directive 95/46 in either its DUP or SRR.

### B. Right of access

Article 12 of Directive 95/46 grants every data subject the right to obtain:

- (1) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- (2) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; and
- (3) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1).<sup>348</sup>

At the bottom of Facebook's 2015 DUP, Facebook indicates that users living outside the US or Canada can contact Facebook with questions regarding its DUP either online or via mail. Individuals who click through on "contact online", will find a form which is intended "*only for questions or clarification related to Facebook's Data Policy (also known as Privacy Policy) or our agreement with TRUSTe*".<sup>349</sup>

---

<sup>346</sup> Facebook, "Accessing Your Facebook Data", accessible at <https://www.facebook.com/help/405183566203254>, last accessed 25 August 2015. It is important to note that this list does not appear in Facebook's DUP.

<sup>347</sup> Cf. *infra*; section 10.B.

<sup>348</sup> Article 12 has been implemented in Belgian law through article 10 BDPA.

<sup>349</sup> Facebook, "Data Policy Questions", accessible at <https://www.facebook.com/help/contact/173545232710000>, last accessed 25 August 2015.

## Data Policy Questions

Name

Your full name

This form is only for questions or clarification related to Facebook's Data Policy (also known as Privacy Policy) or our agreement with TRUSTe. We aren't responding to any other inquiries through this channel. Here are some common things people need help with:

Deactivating or deleting an account

Requesting something be removed from Facebook for privacy law reasons

Requesting a copy of their personal data

One of the links provided is intended for individuals who need help with “*requesting a copy of their personal data*”; which directs users to a page explain how they can make use of the “*Download Your Info*” tool:

### How can I download my information from Facebook?

You can download your information from your [settings](#). To download your information:

1. Click **▼** at the top right of any Facebook page and select **Settings**
2. Click **Download a copy of your Facebook data** below your General Account Settings
3. Click **Start My Archive**

Because this download contains your profile information, you should keep it secure and be careful when storing, sending or uploading it to any other services.

Learn more about [what info is included in your download](#). If you don't have a Facebook account, you can [make a data access request](#).

The “Download Your Info” tool is said to allow users to download a copy of their Facebook data.<sup>350</sup> The file generated through this functionality mainly provides information which is already visible to users when browsing their profile. The file also contains certain additional information, for example, regarding the user's account activity<sup>351</sup> and meta-data linked to uploaded pictures. Facebook additionally provides its users with an “Activity Log”, which provides an overview of the user's actions on Facebook (e.g., posts, likes, check-ins, etc.).<sup>352</sup>

<sup>350</sup> Facebook, “How can I download my information from Facebook?”, accessible at <https://www.facebook.com/help/212802592074644> (last accessed 25 August 2015).

<sup>351</sup> Session information; IP address; browser information; (partial) cookie number.

<sup>352</sup> Facebook, “Explore Your Activity Log”, accessible at <https://www.facebook.com/help/437430672945092> (last accessed 25 August 2015).

In its 2011 Audit, the Irish DPC stated that “*From a transparency perspective, it is desirable that most, and ideally all, of a user’s data should be available without having to make a formal request.*”<sup>353</sup> While improvements have been made, Facebook still does not provide all information it collects about a user through the aforementioned tools. Information which is notably missing, for example, includes certain information collected through websites and apps that use Facebook services (e.g., browsing behavior collected through social plug-ins).<sup>354</sup> Furthermore, neither the “Download Your Info” tool nor the “Activity log” make explicit the actual purposes for which personal data has been used; whom exactly the data has been disclosed to; or the logic behind any automated decision-making or processing.<sup>355</sup>

In conclusion, while Facebook does offer certain voluntary transparency tools, neither its DUP nor its SRR formally recognises the data subject right of access provided under Directive 95/46. Moreover, users may easily get the impression that the more formal “data access requests” are only available to non-users. Finally, the data which are made readily available to users are dispersed over different tools, none of which provide a complete overview of all data collected by Facebook.

### **C. Rights to object and erasure**

The Data Protection Directive provides data subjects with a right to object (article 14) and a right to erasure (article 12(b)). At least with regard to the use of personal data for direct marketing purpose, Facebook’s users should be free to object at any time.<sup>356</sup>

#### **1) Right to object**

Facebook offers its users various means to configure the ability to regulate the visibility of certain information with regard to “Friends”, custom groups or the public at large.<sup>357</sup> Facebook does not offer equally straightforward options to object to the processing of personal data for direct marketing purposes. While certain opt-outs are provided (e.g., Social Ads), there is no ability to opt out for other uses of personal data for direct marketing purposes (e.g., Sponsored Stories, commercial profiling on the basis of their data actively shared on Facebook). Other opt-outs are not provided on-site (e.g. advertising based on activities off of Facebook) but require

---

<sup>353</sup> Data Protection Commissioner, ‘Report of Audit – Facebook Ireland Ltd.’, 21 December 2011, *l.c.*, p. 63.

<sup>354</sup> In 2012, the Irish Data Protection Commissioner noted that such data “*cannot be efficiently retrieved per user*”, citing the technical difficulties identified with extracting information on a specific user from Facebook’s log records (Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, *l.c.*, p. 22). These findings predate Facebook’s 2014 announcement that it would begin using information concerning the browsing activities off of Facebook for advertising purposes by default (cf. *supra*; chapter 8).

<sup>355</sup> See also Maximillian Schrems, *Mag. Maximillian Schrems v. Facebook Ireland Limited*, Handelsgericht Wien, 31 July 2014, p. 36 (paragraph 166-167) [http://www.europe-v-facebook.org/sk/sk\\_en.pdf](http://www.europe-v-facebook.org/sk/sk_en.pdf) (last accessed 3 August 2015).

<sup>356</sup> See also *supra*; Section 2 Consent.

<sup>357</sup> See also *supra*; Section 3 Privacy Settings.

users to navigate a cumbersome opt-out process.<sup>358</sup> Especially in cases where personal data from various services is being combined, simple opt-outs should be provided for processing operations to which the right to object applies.<sup>359</sup>

## 2) Right to erasure

Section IV of Facebook's 2015 DUP states

*"How can I manage or delete information about me?"*

*You can manage the content and information you share when you use Facebook through the [Activity Log](#) tool. You can also download information associated with your Facebook account through our [Download Your Information tool](#).*

*We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.*

*You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates. If you do not want to delete your account, but want to temporarily stop using Facebook, you may deactivate your account instead. To learn more about deactivating or deleting your account, click [here](#). Keep in mind that information that others have shared about you is not part of your account and will not be deleted when you delete your account."*

Facebook's DUP thus presents users with two ways to see personal data deleted: either by manually deleting information which is visible in one's "Activity Log"; or by deleting one's account altogether. Elsewhere, Facebook specifies that when users decide to delete their account, it may take up to 90 days to delete all posted information and "some information (e.g. log records)" might remain in the database for technical reasons.<sup>360</sup>

According to Facebook's DUP, deleting one's profile will result in the deletion of "things you have posted, such as your photos and status updates". Other information (e.g. chat logs, location data, behavioural data) is ostensibly not covered. While the DUP indicates that "information associated with your account" will only be kept "until your account is deleted", it is unclear

---

<sup>358</sup> For example, European users that wish to opt out the use of information regarding their activities outside of Facebook for advertising purposes must (1) navigate to "more settings", (2) select "Adverts", (3) click on the hyperlink of the European Digital Advertising Alliance, (4) select their location, (5) navigate to their ad choices, (6) select the companies one by one and (7) turn off (or scroll down to the setting "turn off all companies"). Cf. supra; section 3.D)

<sup>359</sup> See also CNIL, "CNIL Review of Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data across Services," October 16, 2012. p. 7. See also supra; Section 5.D.4.

<sup>360</sup> Facebook, "How do I permanently delete my account?", accessible at <https://www.facebook.com/help/224562897555674> (last accessed 24 July 2015).

whether “information associated with your account” covers any information other than the information which is immediately visible to users themselves.<sup>361</sup>

Facebook’s DUP makes clear that information posted by other Facebook users will not be deleted automatically when a user requests account deletion. Facebook’s DUP does not, however, make any mention of the data subject’s right to erasure. Facebook’s online contact form (accessible through a hyperlink at the bottom of the DUP) indicates that individuals might actually be able to request certain information to be removed “for privacy law reasons”:



The screenshot shows a form titled "Data Policy Questions". It includes a "Name" field with the placeholder text "Your full name" and an empty input box. Below the input box is a paragraph of text: "This form is only for questions or clarification related to Facebook's Data Policy (also known as Privacy Policy) or our agreement with TRUSTe. We aren't responding to any other inquiries through this channel. Here are some common things people need help with:". Underneath this text are three blue links: "Deactivating or deleting an account", "Requesting something be removed from Facebook for privacy law reasons" (which is highlighted with a red rectangular border), and "Requesting a copy of their personal data".

When clicking through, however, individuals are given the distinct impression that their ability to request the removal of information “for privacy law reasons” only extends to images:

## **How do I request the removal of my image for privacy law reasons?**

If you're trying to request the removal of your image for privacy law reasons, please visit the [image privacy rights](#) section of the Help Center.

In conclusion, Facebook fails to provide explicit recognition of data subject’s right to erasure. Users may easily be misled into thinking that their ability (right) to obtain erasure of data only extends to self-posted content (unless images are concerned) or requires full account deletion.

---

<sup>361</sup> See also Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, *l.c.*, p. 42 (expressing a concern that personal data contained in log files may remain identifiable for up to 90 days).