



SPION

From social media service to advertising network

A critical analysis of Facebook's Revised Policies and Terms

DRAFT 31 March 2015

v1.2



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), the department of Studies on Media, Information and Telecommunication (SMIT) of the Vrije Universiteit Brussel (VUB) (www.smit.vub.ac.be) and the department of Computer Security and Industrial Cryptography (COSIC) of KU Leuven (www.esat.kuleuven.be/cosic). All three departments are part of iMinds (www.iminds.be).

Preface

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

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

PREFACE	2
LIST OF ABBREVIATIONS	6
EXECUTIVE SUMMARY	7
1. INTRODUCTION	9
A. HORIZONTAL EXPANSION	9
B. VERTICAL EXPANSION	9
C. GENERAL ASSESSMENT OF THE REVISED TERMS	10
2. CONSENT	11
A. ROLE OF CONSENT	11
B. REQUIREMENTS FOR VALID CONSENT	12
1) <i>Indication of wishes</i>	13
2) <i>Freely Given</i>	13
3) <i>Specific</i>	14
4) <i>Informed</i>	15
5) <i>Unambiguous</i>	16
3. PRIVACY SETTINGS	17
A. SETTINGS REGULATING ACCESS BY OTHER FACEBOOK USERS	18
B. APPLICATION SETTINGS	19
C. SETTINGS FOR ADVERTISING	21
D. ASSESSMENT	23
4. UNFAIR CONTRACT TERMS	25
A. WARRANTY DISCLAIMER	25
B. LIABILITY LIMITATION	26
C. INDEMNITY CLAUSE	27
D. UNILATERAL CHANGE	27
E. FORUM CLAUSE	29
F. CHOICE OF LAW	30
G. TERMINATION	31
5. HOW FACEBOOK “COMBINES” AND “SHARES” DATA ABOUT ITS USERS	33
A. FACEBOOK’S 2013 DUP	33
B. FACEBOOK’S 2015 DUP	33
C. ASSESSMENT	33
6. LOCATION DATA	36
A. FACEBOOK’S 2013 DUP	36
B. FACEBOOK’S 2015 DUP	37
C. ASSESSMENT	37
7. FURTHER USE OF USER-GENERATED CONTENT	39
A. FACEBOOK’S IP LICENSE	39
B. “SPONSORED STORIES” AND “SOCIAL ADS”	44

1) Unsolicited communications	46
2) Identifying commercial communications	47
3) Right to control the use of one's image.....	49
8. TRACKING THROUGH SOCIAL PLUG-INS.....	52
A. TRACKING OF USERS AND NON-USERS	52
B. FACEBOOK AUDITS 2011-2012.....	53
1) The 2011 Report of Audit.....	53
2) The 2012 Report of Re-Audit.....	54
C. FACEBOOK'S 2013 DUP	55
D. FACEBOOK'S 2015 DUP	56
E. ASSESSMENT.....	57
1) Article 5(3) of the e-Privacy Directive	57
2) Position of the Article 29 Working Party.....	58
3) Facebook's tracking of users	59
4) Facebook's tracking of non-users	60
5) Facebook's proposed opt-out mechanism	61
6) Alternatives	62
9. FINGERPRINTING.....	63
A. FACEBOOK'S 2013 DUP	63
B. FACEBOOK'S 2015 DUP	64
C. ASSESSMENT.....	65
10. DATA SUBJECT RIGHTS	66
A. RIGHT TO INFORMATION	66
B. RIGHT OF ACCESS.....	67
C. RIGHTS TO OBJECT AND ERASURE	67

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 their privacy settings as part of its 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 Part, 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 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 combines 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 smart phone is to do so at the level of the mobile operating system. Facebook should implement a granular 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 mention is made of certain (limited) access rights and opt-out mechanisms, Facebook does not appear to give effect to data subject rights. For example, deleting one's profile is an "all-or-nothing" exercise and only relates to "things you have posted, such as your photos and status updates". Though users have some options to control the visibility of their information within their networks, they are not able to prevent Facebook from further using this information for its purposes.

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")¹ 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 kinds 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.

¹ 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 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/EC², processing of personal data may only take place to the extent that there is a **“legitimate ground”** justifying the processing. The legitimate grounds recognized 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 subject³;
- a necessity for the performance of a contract⁴; and
- an (overriding) legitimate interest⁵.

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”.⁶ 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).⁷ 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.⁸

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 legitimize the processing. For instance, **article 5(3) of the E-Privacy Directive**⁹ entails that OSN providers must obtain the consent of its users prior to:

² 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 of 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”).

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

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

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

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

⁷ *Idem.*

⁸ 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 .

⁹ 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).¹⁰

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/EC 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/EC *de facto* requires users’ consent in order to legitimate these types of processing activities.¹¹ 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.¹²

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.¹³ Where processing is based on consent, individuals in principle also have the right to withdraw consent and to see the underlying personal data removed.¹⁴

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).

¹⁰ 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.

¹¹ 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.

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

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

¹⁴ 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.”¹⁵ 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.”¹⁶

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.¹⁷ 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.”¹⁸

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

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

¹⁶ *Ibid*, p. 12-13.

¹⁷ 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>

¹⁸ 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.¹⁹

3) Specific

In order to be valid, a data subject's consent must relate to clearly identified data and purposes.²⁰ Put differently, the data subject's consent must be clearly and unambiguously given for a specific (category of) purpose(s).²¹ 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'.²² It is unclear, however, to what extent user data is shared with other entities such as 'Facebook Companies', 'Third-Party Partners' and 'Customers', nor what the exact identity is of these entities. 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

¹⁹ 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."*

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

²¹ 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.

²² <https://www.facebook.com/about/privacy/your-info-on-other>

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

4) Informed

*“[T]here must always be information before there can be consent”.*²⁴ Research has shown²⁵ that individuals rarely read privacy notices or general terms of use, let alone understand them.²⁶ 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.²⁷

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”.²⁸ 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.²⁹

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.³⁰ 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.

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

²⁵ 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

²⁶ 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.”)

²⁷ 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.

²⁸ 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.

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

³⁰ 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.

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.³¹

Default settings which are configured to disclose information without the active engagement of the user do not constitute unambiguous consent.³² 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.*”³³

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.³⁴ 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.**

³¹ 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.

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

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

³⁴ 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 who can access their “profile information”.³⁵ Facebook users can either select an audience from a predefined set of groups (e.g., Friends, Friends of Friends, only me, Public), or customise their own audience.

Facebook **has changed its privacy settings many times**. In 2007, 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).³⁶ There was fierce opposition to this service because it functioned on an opt-out basis, meaning that the users had to take active steps to prevent other people from finding out about their off-Facebook activities.³⁷ In 2008, a class action suit was filed against Facebook³⁸ and in 2009, Facebook announced that it would stop the service.³⁹ In 2009, the default settings changed again, resulting in an increase of the data made publicly available by default.⁴⁰ In October 2013, Facebook changed its default settings for teenagers (aged 13-17).⁴¹

Facebook has **not announced any changes to the privacy settings for 2015**. Facebook only introduced its “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 for vis-à-vis advertising or access by third-party application providers.

³⁵ 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. Caviglione et al. (eds), IGI Global, 2012 accessible at <https://lirias.kuleuven.be/bitstream/123456789/373507/1/ACMs%20in%20SNS.pdf>) The terms “profile information” here refers to both basic profile information and additional information that the user adds to his or her profile. It does not concern behavioural profiles created by Facebook for purposes of behavioural targeting.

³⁶ 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>.

³⁷ C. Metz, *Facebook turns out light on Beacon*, 23 September 2009, http://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/.

³⁸ 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>.

³⁹ C. Metz, *idem*.

⁴⁰ 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.

⁴¹ 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 the default settings, the **default configuration** of certain settings **remains problematic**. The following sections will analyse three of the main settings available to Facebook users.

A. Settings regulating access by other Facebook users

Facebook provides several granular settings **regulating access by other Facebook users**. The default regulating access by users is set to “Friends” (for new users⁴²), other possibilities are “Public”, “Friends of friends”, “Custom” and “Only me”.

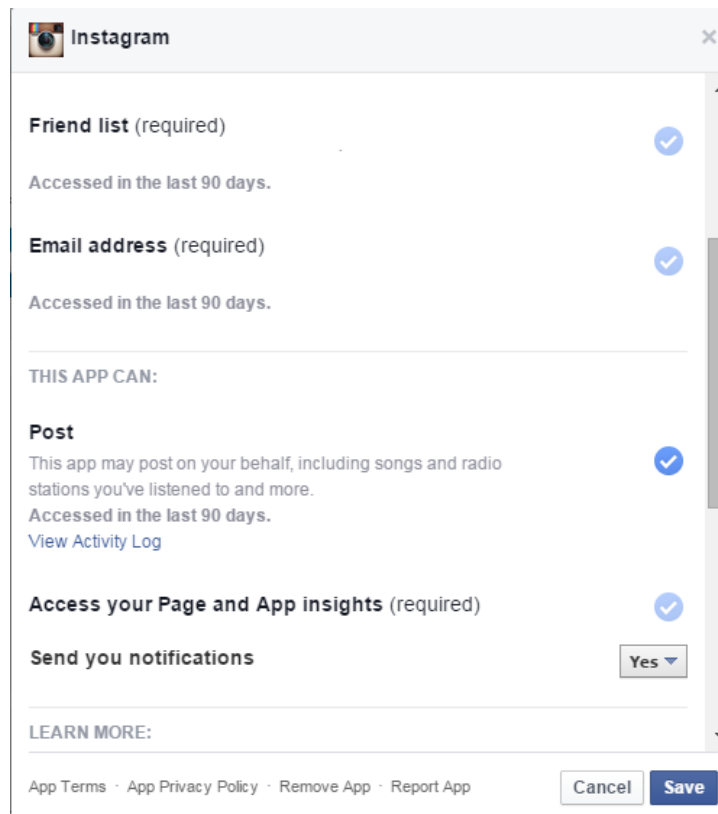
Privacy Settings and Tools			
Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend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

⁴² For existing users the default setting used to be “public”.

In addition, users are able to define the audience for each post separately. When new users post something for the first time, they can select their audience for that particular post. If they don't select anything their info is 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.

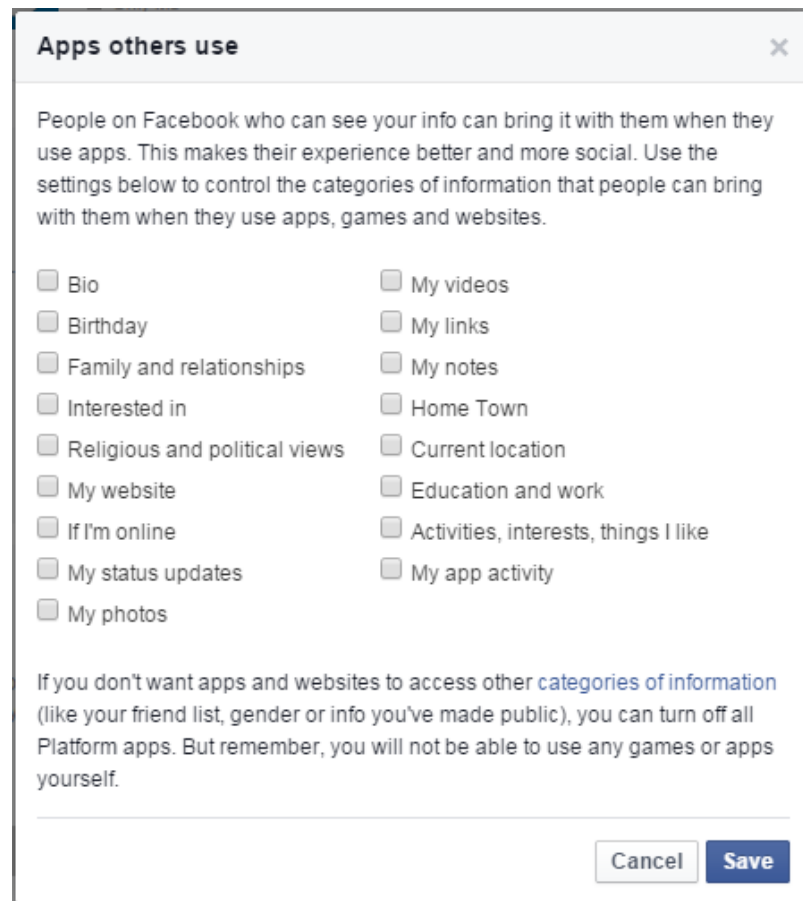
B. Application settings

Facebook also offers **application settings**. 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. The following screenshot shows the application settings for Instagram:



Users are able to change the full blue settings, simply by clicking on it. 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. 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.

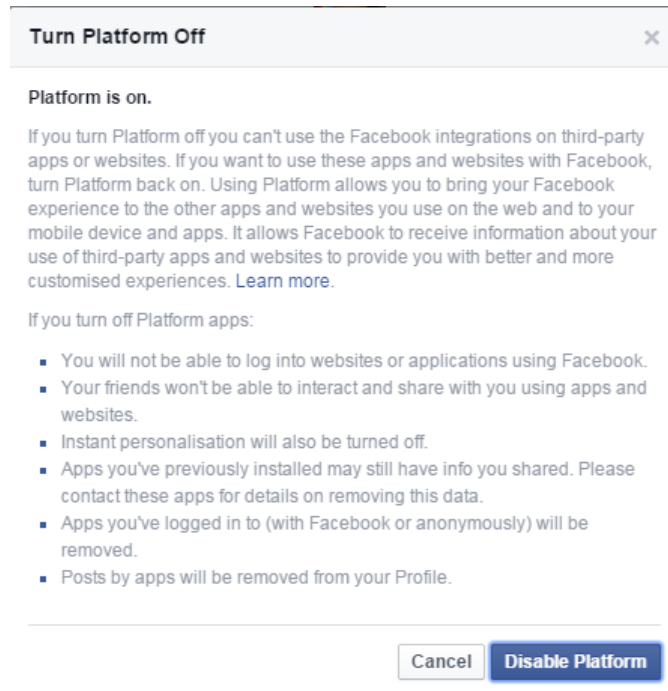
Finally, it is important to note that users can, to a certain extent, allow application providers to **access their friends' data**. Specifically, users can determine which part of their friends' data will be shared with their apps under their app settings.⁴³ Facebook indicates as much under its Apps settings, under the title "Apps other use".



By default, application providers will not have any access to the types of information listed (no boxes are pre-checked). However, application providers will have access to certain categories of information by default (e.g., friend list, gender). 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 that users no longer can make use of "Facebook Login" or "Like" buttons on external websites.⁴⁴

⁴³ A. Hellemond, "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>.

⁴⁴ *Id.*



C. Settings for advertising

The current settings offered for advertising are essentially two-fold⁴⁵. First, users can opt-out from appearing in so-called **Social Ads**. A Social Ad is an ad portraying a brand or Facebook page and the friends who liked it⁴⁶. Users can opt-out from appearing in Social Ads, but cannot opt-out from appearing in so-called “Sponsored Stories”.⁴⁷

⁴⁵ 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 analyse it further for the time being.

⁴⁶ A Social Ad is not the same as Sponsored stories. Sponsored stories attach another story to the fact that someone liked something. Sponsored stories appear in News Feed while social ads appear in a box on the right hand side, designated for advertising.

⁴⁷ See also infra; section 7.B “Sponsored Stories” and “Social Ads”.

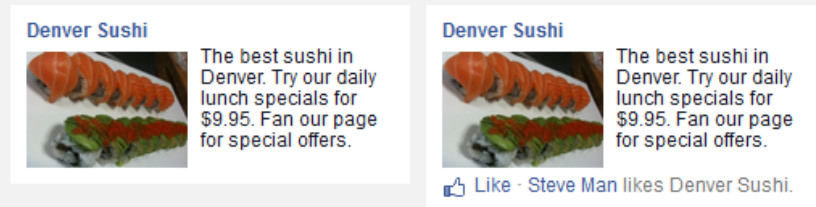
Ads and Friends

Everyone wants to know what their friends like. That's why we pair ads 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 ads](#).

Here are the facts:

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

Here's an example of a Facebook Ad:



This setting only applies to ads that we pair with news about social actions. So, independent 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 ads, Sponsored Stories, and messages from Facebook work in the [Help Center](#).

Pair my social actions with ads for

Save Changes

Cancel

Second, Facebook tells its users they can opt-out of tracking and targeted advertising by providing **links to the websites** of the American, Canadian and **European Digital Advertising Alliance**.

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.

D. Assessment

Adjustable privacy settings can serve as an additional way to obtain consent for certain specific types of data use. 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 OSN should offer default settings⁴⁸

"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".⁴⁹

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.⁵⁰

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 use of data by Facebook itself or by third-parties (e.g., access by application providers or use of personal data for advertising purposes). In other words: users are able to choose from several granular settings which regulate access by other individuals, but cannot exercise meaningful control over the use of their personal information by Facebook or 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.⁵¹

Furthermore if users want to regulate access to their information by apps or the use of data for advertising purposes, they are faced with a rather complicated opt-out system. The Article 29 Working Party has clarified that an opt-out mechanism "*is not an adequate mechanism to obtain average users informed consent*".⁵² As a result, **Facebook's opt-out approach for behavioural profiling and social advertising does not meet the requirements for legally effective**

⁴⁸ 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). Furthermore, concept of privacy by default has also been introduced in the article 23 of the proposed General Data Protection Regulation.

⁴⁹ Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking', *l.c.*, p. 7.

⁵⁰ 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. For example, information contained in a user's profile should not be made available for indexation by (internal or external) search engines unless the user has explicitly agreed to this.

⁵¹ 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>

⁵² Article 29 Working Party Opinion 2/2010 on online behavioural advertising, WP171, 22 June 2010, p. 15.

consent.⁵³ In addition, 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 Stories⁵⁴ or the sharing of location data⁵⁵ with Facebook.

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.⁵⁶ When, in addition, these settings are well hidden and/or hard to adjust, they may also be qualified as “misleading”.⁵⁷ In relation to Facebook’s opt-out mechanism, EDRI has noted that some the language used to instruct users could be misleading and confusing.⁵⁸ Specifically, in one of announcements regarding the revised Terms of Use, Facebook states:

*“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”.*⁵⁹

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).⁶⁰ 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.”*⁶¹

⁵³ Cf. supra; section 2 “Consent”.

⁵⁴ Cf. infra; section 7.B “Sponsored Stories” and “social ads”.

⁵⁵ Cf. infra; section 6 “Location Data”

⁵⁶ 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.

⁵⁷ See art. 6-7 Unfair Commercial Practices Directive; article VI.97 BCEL.

⁵⁸ 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).

⁵⁹ Section “Giving you more control over ads”, <https://www.facebook.com/about/terms-updates>. (last accessed 25 March 2015).

⁶⁰ 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).

⁶¹ *Id.* This process in itself is cumbersome, as it requires the user to navigate to the DAA page, to the Online Ad Choices Page, to the correct country, to the Your Ad Choices page and work out how to opt out of all of the individual companies then a cookie will be placed opting the user out of advertising based on profiling. (*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)⁶², as implemented into national laws.⁶³

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.”⁶⁴

Facebook’s SRR contains a number of provisions which, according to our analysis⁶⁵, violate the UCTD. While these violations were already present in 2013, they are set to persist in 2015.

A. 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*”.⁶⁶ The **blanket warranty**

⁶² 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”).

⁶³ 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, 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>.

⁶⁴ Article 3(1) UCTD.

⁶⁵ 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

⁶⁶ UCTD, Annex 1 (b); Article VI.83, 13° BCEL.

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).⁶⁷

In December 2014, the French Commission for abusive clauses (*Commission des clauses abusives*, CCA), issued a set of recommendations with regard to terms of use of OSN. According to the CCA, warranty disclaimers that do not give the right to reparation for consumer in the event of non-fulfilment by the business of any one of its obligations, are presumed to be unlawful.⁶⁸

B. 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."*⁶⁹

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).⁷⁰ 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

"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.⁷¹

⁶⁷ 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, p. 257.

⁶⁸ 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 (last accessed 18 March 2015).

⁶⁹ 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)

⁷⁰ 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.

⁷¹ See CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, *l.c.*, paragraph 27.

C. 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 in certain jurisdictions.⁷² Moreover, under Belgian law, the recoverability of legal fees is governed by article 1022 the Code of Civil Procedure.⁷³ 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).⁷⁴

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 OSN provider. Any attempt to hold OSN users liable for the fault of the OSN provider may be considered unfair and therefore invalid.⁷⁵

D. Unilateral change

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

⁷² For example, in 2004, a consumer organization 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. 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.

⁷³ 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).

⁷⁴ 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.

⁷⁵ 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, Recommandation 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.

“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.”⁷⁶ This provision of the UCTD has been implemented divergently 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.⁷⁷

It is interesting to note that a German court has invalidated this provision of Facebook’s SRR because of its “significant imbalance”.⁷⁸ 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”⁷⁹ 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 softened the power of unlimited amendment, but this does not, according to the Court, alter the fact that the amendment provision violates German Law.⁸⁰

⁷⁶ UCTD, Annex 1 (j)

⁷⁷ Article VI.83, 2° BCEL.

⁷⁸ Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <http://openjur.de/u/269310.print>.

⁷⁹ 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>).

⁸⁰ Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <<http://openjur.de/u/269310.print>> accessed 9 September 2013. 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.

E. 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 Regulation⁸¹, which lays down the rules for the 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 States within the meaning of article 17(2) of Brussels I.⁸² In any event, Facebook also "directs" its activities to these Member States within the meaning of article 17(c).

⁸¹ 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.

⁸² 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.

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.⁸³ In contrast, the consumer can only be sued in the Member State where he is domiciled.⁸⁴ Parties cannot deviate from it by agreement until after a dispute has arisen and under certain conditions.⁸⁵ This implies that the **forum clause of Facebook's SSR is invalid**.⁸⁶

In addition 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.”⁸⁷

F. 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)⁸⁸ 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

⁸³ 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.

⁸⁴ Article 18(2) Brussels I Regulation.

⁸⁵ 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.

⁸⁶ 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.

⁸⁷ 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.

⁸⁸ 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.

agreement by virtue of the law which, in the absence of choice, would have been applicable (article 6(2) of Rome I).⁸⁹

The French Commission for abusive clauses (CCA) has indicated that choice of law clauses with contents similar to Clause 15(1) of Facebook's SSR 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.⁹⁰

G. 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.⁹¹ 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.⁹² In Belgium, the provision is part of a “black list”⁹³, which provides that any provision which “[...] authorizes a company to terminate an agreement of indefinite time period without a reasonable notice period” shall be **unlawful** (except in case of “force majeure”).⁹⁴ 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 balance between the parties.⁹⁵

⁸⁹ 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.

⁹⁰ CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, 3 December 2014, *l.c.*, at paragraph 46.

⁹¹ Annex article 1 (g) Unfair Terms Directive.

⁹² 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.

⁹³ 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.

⁹⁴ 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.

⁹⁵ CCA, Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux, *l.c.*, at paragraph 36.

Although Germany has not transposed the provision directly, a German court⁹⁶ 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.⁹⁷ 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.⁹⁸

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.*"⁹⁹ 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.¹⁰⁰ 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.

⁹⁶ Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <http://openjur.de/u/269310.print>.

⁹⁷ 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.

⁹⁸ „(1) Dauerschuldverhältnisse kann jeder Vertragsteil aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist kündigen. Ein wichtiger Grund liegt vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zugemutet werden kann. (2) Besteht der wichtige Grund in der Verletzung einer Pflicht aus dem Vertrag, ist die Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung zulässig. § 323 Abs. 2 findet entsprechende Anwendung. (3) Der Berechtigte kann nur innerhalb einer angemessenen Frist kündigen, nachdem er vom Kündigungsgrund Kenntnis erlangt hat.“

⁹⁹ 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.

¹⁰⁰ 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

A. Facebook’s 2013 DUP

“Sometimes we get data from our [affiliates](#) or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.”

B. Facebook’s 2015 DUP

“Information from third-party partners.

We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

Facebook companies.

We receive information about you from companies that are owned or operated by Facebook, in accordance with their terms and policies. [Learn more about these companies and their privacy policies.](#)

Sharing With Third-Party Partners and Customers

We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.”

C. Assessment

To a large extent, the changes introduced by the 2015 DUP are an extension upon existing practices. Nevertheless, the horizontal expansion of Facebook’s processing capabilities creates additional concerns. Facebook combines data from an increasingly wide variety of sources, including an expanded number of “Facebook Services” which are (in principle) also covered by the DUP, and Facebook’s companies (e.g., Whatsapp and Instagram). By combining its sources, Facebook gains a deeper and more detailed view of its users.

Use case: Combining Facebook Data with data from third-party data brokers

Over the past few years, Facebook has partnered with data brokers such as Acxiom, Datalogix and Epsilon so that advertisers can target OSN users on the basis of their purchasing behavior outside the social network.¹⁰¹ Facebook has reportedly also partnered with data broker BlueKai to enable further targeting of Facebook users on the basis of their browsing activities outside of Facebook.¹⁰²

User targeting is achieved through a matching function which can be summarized as follows: a company contacts a data broker with a particular audience in mind (e.g., people interested in losing weight). The data broker then generates a list of email addresses of people it believes that belong to that audience. It then creates a cryptographic hash function for each of the email addresses of each person on the list and sends these hash functions to Facebook. Facebook then compares this list of hash functions to its own list of hash functions of email addresses belonging all Facebook users and then identifies the relevant users as being part of the target group. In case of targeting based on browsing activity, mapping OSN users with the intended audience is done through a process referred to as 'cookie matching'. Even if data brokers do not directly share any data with Facebook other than the relevant hash functions, Facebook might still be able to glean information of the user based on what is being advertised.¹⁰³

As indicated earlier Facebook only offers an opt-out system for its users to regulate the use of their data by third-party 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.

¹⁰¹ Specifically, Facebook has added 'partner categories' as an additional targeting feature, which enables advertisers to target individuals based on the basis of their purchase behaviour outside the social network. See <https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature> (last accessed 17 December 2013). See also C. Dello, 'Facebook to Partner With Acxiom, Epsilon to Match Store Purchases with User Profiles – Can Facebook Ads Drive Offline Buying?', *Advertising Age*, 22 February 2013, available at <http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-store-purchases-user-profiles/239967> (last accessed 7 January 2014).

¹⁰² See K. Opshal and R. Reitman, 'The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads', Electronic Frontier Foundation (EFF), 22 April 2013, available at <https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads> (last accessed 7 January 2014).

¹⁰³ *Id.*

As mentioned earlier, consent cannot be inferred from the data subject's inaction with regard to behavioural advertising. As a result, Facebook's opt-out system for "activity based" advertising does not meet the requirements for legally valid consent (cf. *supra* sections 2 and 3).

6. Location Data

Smart devices contain many sensors which make it possible to determine the location of the person holding it (e.g., GPS, WiFi, etc.).¹⁰⁴ In principle, the operating system of a smart device enables its users to decide whether or not to share location data. When it comes to sharing location data with Facebook, users only have a binary choice: all-or-nothing. Once the Facebook mobile app is authorized to access location data, there are no further (in-app) settings, for example, allowing the individual to authorize location sharing for one purpose but decline it for other purposes.

Even when a user decides to turn off Facebook's access to location data, this still does not prevent Facebook from collecting location data via other means. 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.

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."*

¹⁰⁴ 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.

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... .”

C. Assessment

Facebook's 2015 DUP is slightly more explicit about the types of information Facebook collects in order to locate its user (e.g., the 2015 DUP explicitly also 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.¹⁰⁵ 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).¹⁰⁶ The special nature of location data is also emphasised in article 9 of the e-Privacy Directive¹⁰⁷, providing a specific regime regarding information obligations and consent requirements. Providers of OSNs generally do not qualify

¹⁰⁵ Article 29 Working Party, “Opinion 13/2011 on Geolocation Services on Smart Mobile Devices”, WP185, May 16, 2011, p. 9-11 and 13.

¹⁰⁶ Idem.

¹⁰⁷ 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).

as providers of an “electronic communication service”, meaning Facebook falls largely outside of the scope of the e-Privacy Directive.¹⁰⁸ Nevertheless, a normal reading of article 7 of Directive 95/46 in principle requires informed user consent prior to the sharing of location data.¹⁰⁹

In conclusion, **Facebook should offer granular in-app settings for sharing of location data, with all parameters turned off by default.** This should allow users to determine when, how and what (location) data can be used by Facebook and to what purpose. Additionally, Facebook should provide more detailed information about how, when and why exactly location data is collected. Finally, **location data should only be collected to the extent and for the duration necessary for the provision of a service** requested by the user.

¹⁰⁸ See also Article 29 Working Party, Opinion 5/2009 on Online Social Networking, 12 June 2009, p.10.

¹⁰⁹ See also supra; chapter 2 on the role of consent.

7. Further use of user-generated content

A. Facebook's IP License

Clause 2 of Facebook's 2015 SRR¹¹⁰ 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 way. 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 authorize 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

¹¹⁰ 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 Directive¹¹¹, 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.^{112/113} 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 BCEL¹¹⁴ lists the conditions that are applicable to copyright contracts in general.¹¹⁵ 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 favor 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

¹¹¹ 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.

¹¹² 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>).

¹¹³ 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

¹¹⁴ 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).

¹¹⁵ 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.**¹¹⁶ 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 integrity¹¹⁷ as well as, at least in the so-called *droit d'auteur* countries, the right of divulgation.¹¹⁸ These rights are inalienable as a matter of principle.¹¹⁹ Subject to narrowly defined conditions, it is accepted that a waiver with respect to individual attributes of the moral rights are allowed¹²⁰, 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*¹²¹. 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

¹¹⁶ 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.

¹¹⁷ This obligation results from Article 6bis of the Berne Convention.

¹¹⁸ See, in Belgium, Article 165 § 2 BCEL.

¹¹⁹ Article XI.165 BCEL

¹²⁰ M-Ch. Janssens, “Les droits moraux en Belgique”, *Les Cahiers de propriété intellectuelle* (Canada), vol. 25 n° 1, Janvier 2013, p. 91.

¹²¹ 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).

decision – this is exactly the case, while it is not made explicit in the disputed clause, which 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 with the Facebook IP license is whether its provisions can be qualified as “**unfair**” under the **Unfair Contract Terms Directive (UCTD)**¹²² (*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.¹²³ Second, there must be a significant imbalance to the detriment of the consumer. Third, that imbalance should be “*contrary to good faith*”.¹²⁴ 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.¹²⁵ Furthermore, the Annex to the Directive serves as an indication of which kind of terms could be deemed unfair or not.¹²⁶ Until recently, the CJEU has only provided clarifications regarding the unfairness of specific terms, not the general terms used in article 3.¹²⁷

¹²² Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contract

¹²³ Unfair Terms Directive, art. 3 (2).

¹²⁴ 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.

¹²⁵ Unfair Terms Directive, art. 4 (1).

¹²⁶ 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).

¹²⁷ 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'.¹²⁸ 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.¹²⁹ 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.¹³⁰

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.¹³¹ 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.¹³²

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

¹²⁸ Case C-415/11 *Mohamed Aziz v Catalunyacaixa* [2013].

¹²⁹ *Ibid*, at paragraph 68.

¹³⁰ *Ibid*, at paragraph 69.

¹³¹ Hendrik Vanhees, "Artikel 3", in F. Brison and H. Vanhees (Eds.), *De Belgische Auteurswet. Artikelsgewijze commentaar*, Larcier, Brussel 2012, 32.

¹³² "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.¹³³

B. “Sponsored Stories” and “Social Ads”

Facebook indicates in clause 9 of its 2015 SRR¹³⁴ 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).

¹³³ 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 (last accessed 18 March 2015).

¹³⁴ 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”.*¹³⁵

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”.*¹³⁶

¹³⁵ <https://www.facebook.com/help/214816128640041#Does-Facebook-use-my-name-or-photo-in-ads?>

¹³⁶ 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.”¹³⁷

In a letter to Facebook, the **Norwegian Consumer Ombudsman** characterized 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.”¹³⁸

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).¹³⁹ Given this uncertainty, they argued that such messages should be considered as ‘**other unsolicited communications**’ as defined by Article 13 (3)¹⁴⁰ of the e-privacy Directive and that users must thus be able to opt out of receiving these kind of direct marketing messages.¹⁴¹

Facebook currently **offers neither an opt-in or opt-out** with respect to receiving Sponsored Stories.

¹³⁷ Article 13 of the e-Privacy Directive has implemented in Belgian law by way of articles XII.13 and XIV.77 BCEL.

¹³⁸ 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>.

¹³⁹ 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.

¹⁴⁰ “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.

¹⁴¹ 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.**¹⁴² 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.”*¹⁴³

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.¹⁴⁴

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:



¹⁴² 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.

¹⁴³ 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>

¹⁴⁴ *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).” ¹⁴⁴ 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.¹⁴⁵ 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.



¹⁴⁵ 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.”¹⁴⁶

In principle, anyone seeking to record or use the image of another person must first obtain that person’s consent.¹⁴⁷ In legal terms, the right to control one’s image is sometimes also referred to as the “right of personal portrayal” or “portrait right”.¹⁴⁸ 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.¹⁴⁹ The only requirement to invoke the right of personal portrayal is that the individual is sufficiently identifiable, i.e. can be recognised by others.¹⁵⁰

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).¹⁵¹ 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).¹⁵² 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

¹⁴⁶ European Court of Human Rights, *Reklos and Davourlis v. Greece*, 11 December 2008, at paragraph 40.

¹⁴⁷ D. Voorhoof and P. Valcke, *Handboek Mediarecht*, Larcier, 4^e editie, 2014 p. 239-240.

¹⁴⁸ 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.

¹⁴⁹ 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.

¹⁵⁰ 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.

¹⁵¹ See P. De Hert and R. Saelens, “Recht op afbeelding”, *TPR* 2009, afl. 2, 869.

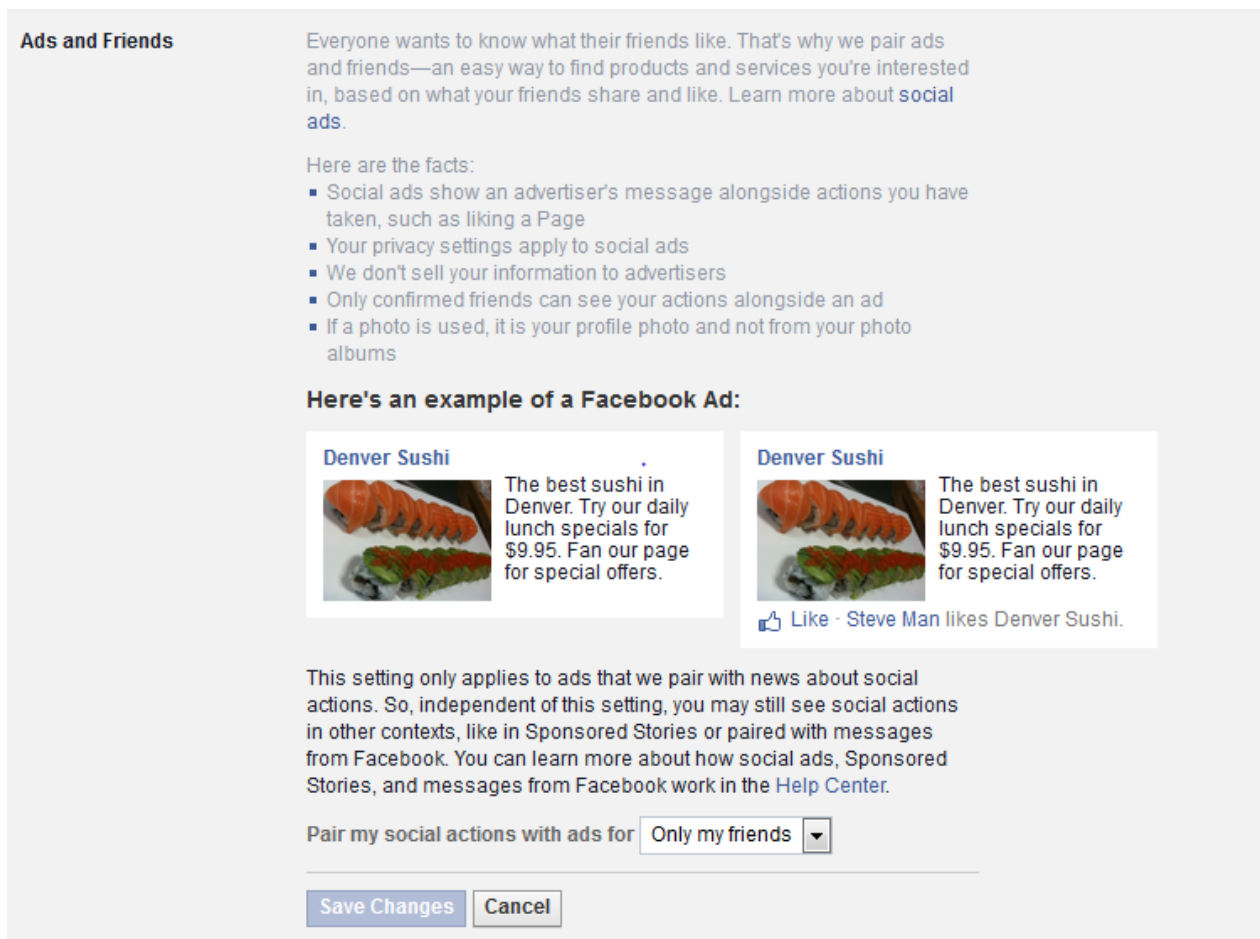
¹⁵² *Id.* For more information see also B. Van Alsenoy and V. Verdoodt, “Liability and accountability of actors in social networking sites”, *SPION* D6.3, December 2014, p. 7 et seq., accessible at www.spion.me.

require the unambiguous, free, specific, informed consent of the individual concerned (cf. *supra*; Section 2 “Consent”).¹⁵³

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:



¹⁵³ 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. 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

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 Story”. 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).¹⁵⁴ 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.¹⁵⁵ For the purposes of this report, we define “**tracking**” as the collection of information about users’ web browsing activities across different websites.¹⁵⁶

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 1.¹⁵⁷

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.¹⁵⁸ 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.¹⁵⁹ Facebook will also receive

¹⁵⁴ 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>.

¹⁵⁵ *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

¹⁵⁶ 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 to 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.

¹⁵⁷ 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 (hereafter: “Annex 1”).

¹⁵⁸ 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.

¹⁵⁹ 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.¹⁶⁰

Facebook's "Like Button", the most popular Facebook social plug-in, is currently present on more than 13 million sites¹⁶¹, covering almost all website categories including health and government websites.¹⁶²

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.**¹⁶³ 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."¹⁶⁴

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.

¹⁶⁰ 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.)

¹⁶¹ <http://trends.builtwith.com/widgets/Facebook-Like> (last accessed 21 March 2015).

¹⁶² 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).

¹⁶³ Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', 21 December 2011, l.c., p. 81-86.

¹⁶⁴ *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”*¹⁶⁵

2) The 2012 Report of Re-Audit

The Irish DPC essentially echoed its 2011 position in the 2012 re-audit.¹⁶⁶ 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*”.¹⁶⁷ 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**.¹⁶⁸ When asked, Facebook informed the technical auditor that the fr cookie “*is being used by Facebook to deliver a series of new advertisement products*”.¹⁶⁹ 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”.¹⁷⁰

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.¹⁷¹ In its annual report for 2012, the Irish DPC indicated that Facebook had satisfied the request for information.¹⁷² 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.

¹⁶⁵ *Ibid*, p. 82

¹⁶⁶ 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).

¹⁶⁷ *Ibid*, p. 28.

¹⁶⁸ 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).

¹⁶⁹ *Ibid*, p. 34.

¹⁷⁰ Data Protection Commissioner, ‘Facebook Ireland Limited – Report of Re-Audit’, 21 September 2012, l.c., p. 28.

¹⁷¹ *Ibid*, p. 7

¹⁷² 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 (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**.¹⁷³ 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 default¹⁷⁴:

*"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."*¹⁷⁵

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."*¹⁷⁶

¹⁷³ 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>"

¹⁷⁴ 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).

¹⁷⁵ 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).

¹⁷⁶ *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.**"¹⁷⁷*

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

¹⁷⁷ 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.¹⁷⁸ 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.

¹⁷⁸ 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).¹⁷⁹ 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.”¹⁸⁰

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.”¹⁸¹

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

¹⁷⁹ 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.

¹⁸⁰ *Ibid*, p. 9

¹⁸¹ *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.¹⁸² 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)"*¹⁸³

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 Facebook¹⁸⁴, 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 criticized extensively. First, it has been argued that certain language used by Facebook

¹⁸² 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.

¹⁸³ See <https://www.facebook.com/help/cookies> (last accessed 22 March 2015)

¹⁸⁴ 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. TACD¹⁸⁵ and EDRI¹⁸⁶). 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.¹⁸⁷ This means that **Facebook’s current opt-out approach does not satisfy the requirements for legally valid consent**.¹⁸⁸ 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.¹⁸⁹

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.¹⁹⁰

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

¹⁸⁵ 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)

¹⁸⁶ 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/>

¹⁸⁷ Article 29 Working Party Opinion 2/2010 on online behavioural advertising, *l.c.*, p. 15.

¹⁸⁸ 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. 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”

¹⁸⁹ 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).

¹⁹⁰ 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.¹⁹¹ 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*.¹⁹² 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.¹⁹³ 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.¹⁹⁴ 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 users¹⁹⁵, one for Canadian users¹⁹⁶ and one for US users¹⁹⁷.

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 2012.¹⁹⁸

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.¹⁹⁹ All subsequent visits to pages including Facebook social plug-ins can be tracked and linked by Facebook using this cookie

¹⁹¹ 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.*"

¹⁹² 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.

¹⁹³ Article 29 Data Protection Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *l.c.*, p. 7

¹⁹⁴ See <https://www.facebook.com/about/ads> (last accessed 23 March 2015). See section 6.1.1 of Annex 1.

¹⁹⁵ <http://www.youronlinechoices.eu>

¹⁹⁶ <http://youradchoices.ca/>

¹⁹⁷ <http://www.aboutads.info/choices/>

¹⁹⁸ Cf. *supra*; section 8.B.2)

¹⁹⁹ 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.**²⁰⁰

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.²⁰¹ 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.²⁰² The French Data Protection Authority (CNIL) has in fact endorsed this approach as a means to achieve compliance.²⁰³

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.²⁰⁴ 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.

²⁰⁰ <http://www.aboutads.info/choices>; <http://youradchoices.ca>. See section 6.2.2 of Annex 1.

²⁰¹ For more information see <http://panzi.github.io/SocialSharePrivacy/>

²⁰² Id.

²⁰³ 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>

²⁰⁴ 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.²⁰⁵ 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.²⁰⁶

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.).²⁰⁷ 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.²⁰⁸ 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.”

²⁰⁵ 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. 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.

²⁰⁶ 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.

²⁰⁷ 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 and O. Tene and J. Polonetsky, “To Track or “Do Not Track”, *l.c.*, p. 295.

²⁰⁸ 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".²⁰⁹ **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**.²¹⁰ Moreover, there is a new subsection²¹¹ 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 the 2015 DUP, 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.

²⁰⁹ <https://www.facebook.com/about/privacy/cookies>

²¹⁰ 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.*"

²¹¹ 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).”*²¹²

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).²¹³

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).

²¹² 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.

²¹³ 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) a right to information; (b) a right of access and (c) right to object and to erasure.

A. Right to information

Articles 10 and 11 of Directive 95/46 specify certain **types of information** data controllers must provide to data subjects with regards to the processing of their personal data.²¹⁴ 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.²¹⁵ In addition, the Directive offers Member States the option to 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.²¹⁶

Facebook’s DUP provides a broad overview of the purposes for which it processes personal data. This overview, however, is extremely generic and **encompasses all data** collected by Facebook. As a result, it is extremely difficult for any individual to ascertain to which uses specific data are actually being put. Moreover, the **list of potential recipients is not clear at all**. While the concept of “Facebook Services” is explicitly defined, other key concepts such as “partners” are not defined at all. Finally, other than in the manner and form described below, Facebook **fails to make any explicit mention of the data subject rights** of European users.

²¹⁴ 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. Both provisions have been implemented into Belgium law through article 9 BDPA.

²¹⁵ 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 (last accessed on 23 March 2011), commenting on the relevant provision of the German Data Protection Act, which uses the term “purposes” as well.

²¹⁶ 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.

B. Right of access

Article 12 of the Directive grants data subjects the right to obtain certain information. This includes information on the (specific categories) of data that are being processed and for what purposes; where the data comes from; and how it is used for automated decision making.²¹⁷

Facebook provides a tool to its users for downloading their data. The information file generated through this functionality, however, only concerns the requestor's own profile (which only constitutes a fraction of the data Facebook holds on individuals).²¹⁸ It also does not make explicit the actual purposes personal data has been used for; whom exactly the data has been disclosed to; nor the logic behind any automated decision making. Moreover, the information is communicated in one large pdf file. This practice further reduces the practical utility of the information.²¹⁹

C. Rights to object and erasure

As to **data subject's rights to object and to erase**, it is not clear to what extent they can effectively be exercised. 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.²²⁰

Facebook offers users the ability to 'permanently delete' their account. The OSN specifies that this process might take up to 90 days and "*some information (e.g. log records)*" might remain in the database for technical reasons.²²¹ According to Facebook's DUP, deleting your profile will only result in the deletion of "things you have posted, such as your photos and status updates". Information posted by others, cannot be deleted by the respective data subject.²²²

In conclusion, Facebook fails to provide (sufficient) granularity in exercising data subject's rights. For example, the right to erasure can only be exercised with regard to the user's profile altogether and only relates to self-posted content. The right to object can only be exercised with regard to the visibility of certain content to third parties. Finally, all of these rights are only mentioned implicitly (and scattered out) in Facebook's DUP.

²¹⁷ Article 12 has been implemented in Belgian law through article 10 BDPA.

²¹⁸ See *Europe v. Facebook*, "Get your Data! Make an Access Request at Facebook!", at http://www.europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html. Other data includes inter alia: "pictures, postings, videos, events, messages, relationships, data from external sources and an unknown amount of meta-data."

²¹⁹ A non-machine-readable pdf document of hundreds of pages makes it incredibly hard for individuals to understand the full scope of the information.

²²⁰ See also *supra*; Section 2 Consent.

²²¹ <https://www.facebook.com/help/224562897555674>.

²²² "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."