Belgium

Facebook Loses the First Round of Its Battle with the Belgian Privacy Commission

*Stéphanie De Smedt**

I. Background

1. It all started in February 2015. University researchers, commissioned by the Belgian Privacy Commission, published a report containing a legal analysis, under Belgian law, of Facebook's revised terms of use and privacy policy. Facebook had applied them as from 30 January 2015.[1] These revised terms allowed Facebook to track both users and non-users across websites and devices, by using social plug-ins and cookies. In particular, by using the so-called 'datr' cookie, Facebook was able to monitor both users and non-users in a variety of ways, on and off Facebook.[2] The academic research report concluded that these 'tracking' activities violated both European and Belgian data protection legislation.[3]

2. On 13 May 2015, the Privacy Commission issued a formal recommendation. It criticised Facebook's tracking activities, and it formally requested Facebook to cease these activities.[4] Although recommendations of the Belgian Privacy Commission are not legally binding, they should *de facto* be obeyed in order to avoid non-compliance issues.

According to the Privacy Commission, Facebook's tracking activities are more intrusive than other cases of so-called 'third-party tracking'. It is indeed able to track surfing behaviour over a large number of websites, and to link this surfing behaviour to users' real identity, social network interactions and even their medical information and religious, sexual and political preferences. To justify its collection of data through social plug-ins, Facebook relies upon the individual's consent. The Privacy Commission, however, concluded that the conditions for valid (free and informed) consent were not met, and that there was no legal ground for Facebook's tracking activities, particularly when it came to the tracking of non-users.

3. After several months of negotiations, it was clear that no amicable solution could be found. The Privacy Commission consequently sued Facebook before the President of the Brussels Court of First Instance in summary proceedings. The relief sought was an injunction prohibiting the use by Facebook of the 'datr' cookie through social plug-ins to track non-users, without first giving them sufficient and adequate information in this re-

* Associate with Loyens & Loeff Brussels (Belgium), specialising in intellectual property and information technology law (including privacy and data protection). For correspondence: <stephanie.de.smedt@loyensloeff.com>.

1 See academic report '*From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms*', version 1.3 https://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation accessed 13 December 2015.

2 See technical '*report on Facebook tracking through social plug-ins*', written by KULeuven and iMinds researchers at the request of the Belgian Privacy Commission https://secure-homes.esat.kuleuven.be/~gacar/fb_tracking/ accessed 13 December 2015. The 'datr' cookie is a long-term (lifespan of 2 years), uniquely identifying tracking cookie sent to Facebook when a site with Facebook social plug-ins is visited by logged-in, logged-out or deactivated Facebook users alike. In addition, also when a non-user visits a Facebook page (event page, fan page, etc.), visits certain third-party websites, or opts-out from interest-based advertising on the European Digital Advertising Alliance website, the 'datr' cookie is set. All later visits to sites that include Facebook social plug-ins can consequently be tracked and linked by Facebook. The proclaimed purpose of the 'datr' cookie is website security and integrity maintenance.

3 The Belgian law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data (BDPA) implements EU Data Protection Directive 95/46/EC of 24 October 1995 in the Belgian legal order. Additionally, Article 129 of the Electronic Communications Act of 13 June 2005 (ECA) implements in the Belgian legal order the provisions relating to the use of cookies of EU Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive 2002/58/EC).

4 Recommendation no. 04/2015 of 13 May 2015 (*in English*) <http://www.privacycommission.be/sites/privacycommission/files/documents/recommendation_04_2015_0.pdf> accessed 13 December 2015.

spect.[5] The Privacy Commission sued the US parent company, Facebook Inc., its Irish subsidiary, Facebook Ireland Ltd., and its Belgian subsidiary, Facebook Belgium SPRL/BVBA (together 'Facebook').

4. On 9 November 2015, the President of the Brussels Court of First Instance (the Court) pronounced its long-awaited judgment. The President sided with the Belgian Privacy Commission, and ordered Facebook to stop tracking non-users in Belgium within 48 hours as from the service of the judgment. Facebook was also made subject to penalty payments of €250.000 for each day of continued infringement.[6] Facebook has already announced that it will appeal this judgment.[7] The appeal will not, however, suspend any penalties from becoming due. They are indeed immediately enforceable once the judgment is officially served on Facebook.

II. Key Findings of the President of the Brussels Court of First Instance

1. Territorial Scope of Application of the BDPA

5. A much debated issue in this case was the territorial application of the BDPA and the international jurisdiction of the Belgian courts. Article 3bis of the BDPA (implementing Article 4 of Data Protection Directive 95/46/EC) defines the territorial scope of application of the BDPA as follows:

> This law shall apply to:
> 1° the processing of personal data carried out in the context of the effective and actual activities of a permanent establishment of the controller on Belgian territory or on a place where Belgian law applies by virtue of international public law;
> 2° the processing of personal data by a controller who has no permanent establishment on the territory of the European Community, if for purposes of the processing use is made of equipment, automated or otherwise, situated on Belgian territory, unless such equipment is used only for purposes of transit over the Belgian territory. (...)

Additionally, Article 4(1)(a) of EU Data Protection Directive 95/46/EC makes it clear that, when a data controller is established in the territory of several Member States, it must take the necessary measures to ensure that each of those establishments complies with the obligations laid down by the applicable national law.

6. As its European headquarters are located in Ireland, Facebook argued that the Irish entity, Facebook Ireland Ltd. had to be regarded as the data controller as far as European data processing was concerned. Facebook Ireland, and not Facebook Inc., actually offers the Facebook service to EU users. According to Facebook, there are meaningful differences between the services offered by Facebook Inc. in the United States and Canada, and those offered by Facebook Ireland in the EU and the rest of the world. Consequently, only the Irish data protection legislation would apply and only the Irish courts would have jurisdiction over non-compliance matters.

The Court disagreed, and found that the BDPA does apply in certain cases where an international group does not have its main European establishment in Belgium. In this case, the application of the BDPA was deemed to be triggered by the finding that the activities of Facebook Belgium SPRL/BVBA (the permanent Belgian Facebook establishment) serve and promote the commercial interests and activities of the entire Facebook Group relating to its social networking and advertising activities, and are, therefore, inextricably linked to those of Facebook Inc. (cf

5 The Privacy Commission limited its claim to the tracking of non-users only. It did not (at this stage) request any injunctive relief with respect to the use of the 'datr' cookie for the tracking of Facebook users. In the subsequent procedure on the merits (the introductory hearing is scheduled to take place early January 2016), the Privacy Commission can (and will probably) extend its claim, and request the prohibition of the use of the 'datr' cookie for the tracking of both non-users and users alike.

6 An (unofficial) English translation of the judgment is available on the Belgian Privacy Commission's website, via the following link: <https://www.privacycommission.be/en/news/judgment-facebook-case> accessed 13 December 2015.

7 On the date this article was submitted by the author, no appeal was introduced, yet. Facebook was still negotiating the (provisional) implementation of the judgment with the Belgian Privacy Commission. The Privacy Commission has however already announced that it considers the provisional measures that have in the meanwhile been implemented by Facebook (blocking access to pages for non-users and requiring non-users to log in to be able to view public Facebook pages) to be excessive and, in their turn, contrary to each individual's fundamental right to information. The Privacy Commission has therefore given instructions to proceed with the service of the judgment on the different Facebook entities involved. On the date this article was submitted, the service had however not yet taken place.

ground 1° above).[8] Incidentally, the Court was of the opinion that ensuring relations with public authorities and lobbying activities carried out by a Belgian establishment are also activities which are intended to make the service offered by a social network, profitable, so that they are, by definition, inextricably linked to the activities of the foreign operator of the social network site.

The court agreed with the Privacy Commission's argument that, in this case, it is irrelevant, whether the controller is Facebook Inc. or Facebook Ireland Ltd, for the purpose of determining the applicable law. Both are part of the Facebook Group, as is the Belgian establishment, Facebook Belgium SPRL/BVBA.[9] Also the country where the actual processing takes place, is of no importance in this respect.

2. The Condition of Urgency Is Deemed to Be Automatically Met in Cases of Violation of the Fundamental Right to Privacy

7. In Belgium, in order to obtain injunctive relief through an interim judgment, claimants have to demonstrate 'urgency' (i.e. a situation where the fear of damage of a certain scope, or of serious inconvenience, requires an immediate decision).[10]

According to the Court, a claim relating to a violation of basic rights and freedoms (fundamental rights) by the defendant, is always urgent. Such is even more so in this case, as the alleged violation related not only to an individual's fundamental rights, but to those of a large swathe of the population, and concerned potentially highly sensitive information.

3. IP Addresses Are 'Personal Data'

8. Facebook had argued that IP addresses could only be used to identify computers, and not individuals. They would, therefore, not constitute 'personal data' within the meaning of the BDPA. The data collected by the 'datr' cookie would only contain anonymous IP address details. It would not be possible for a website operator to identify or single out an individual non-registered user based on this information alone. In the absence of such processing of 'personal data', the BDPA would, according to Facebook, not apply.

The Court refuted this argument. It found that the 'datr' cookie uniquely identifies the browser of an Internet user, enabling Facebook to directly or indirectly identify individuals by means of the IP address of their computer. Following the opinions of the Article 29 Working Party[11], and in line with the jurisprudence of the Court of Justice of the EU[12], the Court expressly confirmed that the collection of website visitors' IP addresses through cookies or social plugins, qualifies as the 'processing of personal data' within the meaning of the BPDA and EU Data Protection Directive 95/46/EC.

4. No Adequate Legal Basis for the Tracking of Non-Users

9. *First*, the processing of personal data is only authorised if the data controller can rely on a legitimate basis[13], such as (i) the fact that the processing is necessary for the performance of a contract to which the data subject is a party, (ii) the necessity of the processing in order to meet a legal obligation, (iii) the necessity of the contested processing to promote the legitimate interests of the data controller (except where such interests are overridden by the interests

8 Facebook Belgium SPRL/BVBA is a limited-liability company under Belgian law, incorporated in 2001. In Facebook Belgium's annual financial statement, Facebook Inc. is mentioned as the 'consolidating parent company'. Additionally, pursuant to its deed of incorporation, Facebook Belgium's activities are intended to serve and promote the commercial interests and activities of the entire Facebook Group relating to its social network and advertising activities. Moreover, two members of staff of Facebook Belgium were found to be in contact with Belgian enterprises to provide support services relating to the marketing and sale of advertising space by Facebook Ireland Ltd.

9 See recital 19 of the preamble of EU Data Protection Directive 95/46/EC: 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements (...). The legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect'.

10 See Belgian Court of Cassation, judgments of 21 March 1985 (*Arr.Cass.*, 1984-85, 1008), 21 May 1987 (*Arr.Cass.* 1986-87, 1287), 11 May 1990 (*R.W.* 1990-91, 987), and 13 September 1990 (*Arr. Cass.* 1990-91, 42).

11 See Art 29 WP Opinion no. 4/2007 of 20 June 2007 on the concept of personal data and Art 29 WP Opinion no. 1/2008 of 4 April 2008 on data protection issues related to search engines. See also Art 29 WP Working Document of 21 November 2000, 'Privacy on the Internet - An integrated EU Approach to On-line Data Protection'.

12 Case C-70/10 *Scarlet Extended SA. vs. SABAM* (CJEU, 24 November 2011) recital 51. See also the preliminary reference currently pending before the CJEU, Case C-582/14 *Breyer* (question referred to the CJEU by the German Federal Supreme Court: 'Must

or fundamental rights and freedoms of the data subject), and (iv) the data subject's prior express consent. In addition, pursuant to Article 129 ECA[14], the legality of the systematic placement of non-technical cookies and social plugins on Internet users' computers or devices always requires prior, free, informed and unambiguous consent.

In the case at hand, it was clear that Facebook did not have a contractual relationship with non-users (who had never created a Facebook account and had never accepted Facebook's general terms and conditions). It was also clear that Facebook had no legal obligation under any law to use the 'datr' cookie. With respect to the 'legitimate interest' argument, the Court held that it is not very credible that requesting the 'datr' cookie every time a social plug-in is loading on a website visited by a non-user of Facebook, is actually necessary to ensure the security of Facebook services, especially since criminals can very easily circumvent the placing of this cookie with cookie blocker software. The contested processing was thus deemed to lack the necessary efficacy to achieve its alleged security purpose. The Court concluded that when the interests of Facebook are weighed against the fundamental rights of the affected non-users, the latter's interests undeniably prevail.

Finally, with respect to the alternative legal basis of consent, the Court again sided with the Belgian Privacy Commission. It held that the conditions for valid consent[15] had not been met.

Facebook argued that it only placed the 'datr' cookie with non-users when they explicitly interact with the Facebook service (i.e. actively choose to visit a website of the facebook.com domain or to interact with a Facebook plug-in on a third-party website). It claimed that it would not, therefore, apply the 'datr' cookie as a third party, but based on the express consent of the relevant data subjects. The debate before the Court also showed that, since the summons was issued, Facebook had started to deploy a cookie banner throughout the EU, including Belgium, for non-registered users. The cookie banner was, according to Facebook, deployed in the EU to enhance the consent granted by EU Internet users when they interact with the Facebook service. Facebook stated that, if the non-user leaves the Facebook page without consenting to the placement of cookies, or merely follows the link to learn more information about these cookies, no cookie is placed. Facebook would consequently obtain adequate prior data subject consent before placing the 'datr' cookie.

The court however followed the Privacy Commission's argument to the contrary. It held that, in the case of Internet users who had never registered on Facebook, nor validly accepted Facebook's terms of use, but who had landed on the facebook.com domain (which resulted in the placing of the 'datr' cookie), Facebook had failed to show that it was authorised to place this cookie. The Court also considered that the recently implemented cookie banner did not amount to valid and unambiguous consent. Moreover, according to the Court, a non-user of Facebook who once visited the facebook.com domain can hardly be qualified as a 'user' who explicitly requests a Facebook service every time he/she visits a third-party website on which a social plug-in has been placed.

10. *Secondly*, as a general rule, pursuant to Article 4 BDPA[16], data processing activities must be always adequate, relevant and not be excessive (i.e. limited to what is strictly necessary in order to achieve specific purpose(s)). Facebook argued that the data collected by the disputed 'datr' cookie are only kept for a period of time which is long enough to actually ensure security. The 'datr' cookie would play a crucial role in the protection of the Facebook service against a whole series of security threats, to the benefit of both users and non-users.

The Court again disagreed. It held that, since the personal data of non-users can already be processed before these non-users are able to obtain complete information, or do not even wish to use the social plug-in or more generally the Facebook services, this data is seemingly not processed fairly and lawfully, and it is not obtained for specified, explicit and legitimate purposes. Moreover, there appear to be less intrusive methods to achieve the desired security purpose, with the result that the data processing complained of fails the proportionality test as well.

Article 2(a) of Directive 95/46/ [...] be interpreted as meaning that an Internet Protocol address (IP address) which a service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?').

13 Art 5 BDPA (cf Art 7 EU Data Protection Directive 95/46/EC).

14 Implementing Art 5(3)(e) of Privacy Directive 2002/58/EC.

15 See requirements for valid consent described in Art 29 WP Opinion no 15/2011 of 13 July 2011 on the definition of consent.

16 Cf Art 6 EU Data Protection Directive 95/46/EC.

III. Comments

1. Broad Territorial Application of EU Data Protection Legislation

11. For Facebook and other international companies with multiple establishments in the EU, this judgment confirms that multiple national data protection laws may apply, and must be complied with, and not just the data protection laws of the group's main European establishment.

In reaching its decision, the Court relied on the first ground (1°) of Article 3bis BDPA (activities of a permanent establishment of the US data controller on the Belgian territory – see above). [17]

In our view, as also put forward by the Belgian Privacy Commission in its formal recommendation of 13 May 2015, the Court could alternatively have relied on the second ground (2°) of Article 3bis BDPA:

> the processing of personal data by a data controller who has no permanent establishment on the territory of the European Community, if for purposes of the processing use is made of equipment, automated or otherwise, situated on Belgian territory, unless such equipment is used only for purposes of transit over the Belgian territory

In fact, as a data controller established in the US, Facebook Inc. makes use, for the purpose of data processing, of 'equipment' (the computers and devices on which cookies and social plug-ins are stored[18]) located on the Belgian territory.

12. Under the current EU data protection regime, it is thus perfectly possible that a company with establishments in several Member States, or even a company with no EU establishment, which uses "equipment" located on the territory of one or more Member States, is subject to the regulatory powers of several national data protection authorities. The latter do not all offer the same level of protection, even though they implement the same EU Directive. International groups would be well advised to take the necessary measures to ensure that each of their EU establishments meets the obligations imposed by the applicable national data protection legislation.

The aim of the proposed General Data Protection Regulation (GDPR) is to accommodate this legal uncertainty by creating a single EU data protection law and harmonising its national application by stronger cross-border cooperation. In addition, the ongoing debate about the 'one-stop shop' mechanism is particularly relevant for large multinational companies like Facebook, as such mechanism enables them to deal with only one data protection authority and to simplify their non-compliance risk assessments.

2. Reasoning Also Applies to the Tracking of Non-Users

13. For the purpose of the present interim proceedings, the Privacy Commission limited its claim to the tracking of non-users of Facebook. In the procedure on the merits (which has already been initiated) the Privacy Commission will most likely extend its claim to the tracking of Facebook users.

In our view, the same principles should apply to the use of the 'datr' cookie for the tracking of Facebook users. Even though they have subscribed to Facebook's terms of service, it will not be easy for Facebook to demonstrate that the conditions for a valid opt-in consent have been met.[19] *First*, data sub-

17 Cf the *Google Spain* case (Case C-131/12 *Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos and Mario Costeja González* (CJEU, 13 May 2014)). In this case, the CJEU held that Art 4(1)(a) of Directive 95/46/EC is to be interpreted as meaning that processing of personal data is 'carried out in the context of the activities of an establishment of the controller on the territory of a Member State', within the meaning of that provision, when the operator of a search engine sets up, in a Member State, a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State; cf on this case detailed comment of Kranenborg, 'Google and the Right to Be Forgotten' (2015) 1 EdpL 70. The broad scope of application of the EU data protection legislation was recently also confirmed in the *Weltimmo* case (Case C-230/14 *Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság* (CJEU, 1 October 2015)). Here the CJEU found that the presence of only one representative in a Member State can, in some circumstances, suffice to trigger the applicability of that Member State's national data protection legislation, if that representative acts with a sufficient degree of stability for the provision of the services concerned in the Member State in question; cf extensive case comment by Cole and Giurgiu, 'The 'Minimal' Approach: the CJEU on the Concept of 'Establishment' Triggering Jurisdiction for DPAs and Limitations of Their Sanctioning Powers' (2015) 4 EdpL 310.

18 Cf Art 29 WP Opinion no. 8/2010 of 16 December 2010 on applicable law and Art 29 WP Opinion no. 8/2014 on the Recent Developments on the Internet of Things, applying a very broad definition of the term 'equipment'.

19 See academic report 'From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms', version 1.3 (n 2) and the Belgian Privacy Commission's Recommendation no. 04/2015 of 13 May 2015 (n 5).

jects must be given a 'real choice'. Both Facebook's dominant position in the social network market and the fact that choices are very limited, could undermine the element 'free choice', which is essential to the consent that Facebook would need. *Secondly*, no 'specific' consent is requested for Facebook's commercial profiling activities (users' consent to the general terms and conditions is rather vague and generally worded). *Thirdly*, in the present case, the Court has already found that data subjects received insufficient information from Facebook for them to be able to give their 'informed' consent. *Finally*, settings which have been preconfigured in such a way that personal data is unnecessarily disclosed, without the user having actively consented (i.e. an 'opt-out' approach), arguably do not satisfy the requirement of 'unambiguous' consent. The Privacy Commission has already pointed out that it also considers Facebook's tracking of users to be excessive, especially in the case of logged-out or deactivated Facebook users.

3. Companies Should Be Careful When Using Social Plug-Ins on Company Websites

14. Many website owners do not realise that, as from the moment they implement social plug-ins (allowing their website's visitors, among others, to share content with their social network by posting a reaction or 'liking' an article) and collect IP addresses, they are subject to the application of European data protection legislation.

In its formal recommendation of 13 May 2015, the Belgian Privacy Commission has already warned website owners and webmasters who use Facebook's social plug-ins, of their legal obligation to properly inform visitors to their websites of the types of cookies and plug-ins they are using, the information they are collecting, the purposes for which this information is used, and the length of storage of the cookie/plug-in on the Internet users' computer/device. In addition, for most types of cookies and plug-ins (including Facebook plug-ins), website owners must obtain Internet users' prior express consent before they are activated. The implementation of a generic banner that still leaves room for ambiguity as to the Internet users' actual intentions, will not suffice to escape liability under the BDPA and Article 129 ECA.

IV. Outlook

15. Previously, the Belgian Privacy Commission preferred to stay in the background. It has now however taken it upon itself to bring court proceedings against US giant Facebook for non-compliance with the BDPA. It is not yet clear if the Privacy Commission's decision to actively pursue Facebook is a one-off showcase initiative, prompted by the specific nature of the alleged infringer and its activities, or the beginning of a new era of active enforcement.[20] This will largely depend on the Belgian government's further commitments and on the budget and human resources made available to the Privacy Commission for compliance, monitoring and prosecution purposes. In any event, following this judgment and similar cases in other EU Member States, showing a trend (which is likely to become more marked after the adoption of the GDPR and the increase in sanctions for non-compliance), companies would be well advised to thoroughly review their data protection compliance status.

20 In any case, the Belgian Privacy Commission will soon enough be confronted with Facebook again, now that Max Schrems has requested the Irish, Belgian and German data protection authorities to investigate and suspend Facebook's data transfers to the US following the invalidation of the EU-US Safe Harbour framework.