[logo]

Number of the Divisional Court 222
Repository Number **2015/**
Date of the decision: **9 November 2015**
Case List Number **15/57/C**

222
s. pr.
15

☐ Not to be filed with the tax collector

DUTCH-SPEAKING COURT OF FIRST INSTANCE BRUSSELS

Decision

Division of Summary Proceedings
Temporary Measures
Art. 584 of the Judicial Code

Filed on
Not to be registered

In the case of:

Mr **Willem DEBEUCKELAERE**, pursuant to Article 32, § 3 of the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, acting in his capacity of **PRESIDENT OF THE BELGIAN COMMISSION FOR THE PROTECTION OF PRIVACY**, with enterprise number 0893.076.921, set up at the House of Representatives pursuant to Article 23 of the aforementioned Act of 8 December 1992, established rue de la Presse 35, 1000 Brussels, Belgium, where he elects residence,

Plaintiff,
Represented by Mr Frederic Debusseré, Mr Jos Dumortier and Mr Roex, lawyers in 1000 Brussels, rue du Congrès 35;

Versus:

1. The company under the law of the State of Delaware (United States of America) **FACEBOOK INC.**, with establishment located 1601 Willow Road, CA 94025 Menlo Park, United States of America,

First defendant,
Represented by Mr Dirk Van Liedekerke, lawyer in 1050 Brussels, avenue Louise 326;

2. **FACEBOOK BELGIUM SPRL**, with Registered Office in 1040 Brussels, Rond-Point Schuman 11, with enterprise number 0836.948.464, RPR (Register of Legal Persons) Brussel,

Second defendant,
Represented by Mr Dirk Lindemans, lawyer in 1000 Brussels, boulevard de l'Empereur 3, in his own name and on behalf of Mrs Henriette Tielemans, lawyer in 1040 Brussels, avenue des Arts 44;

3. The company under Irish law **FACEBOOK IRELAND LIMITED**, with Registered Office located 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, 216410, Ireland, with enterprise number 462932,

Third defendant,

Represented by Mr Paul Lefebvre, lawyer in 1050 Brussels, avenue Louise 480;

++++++++++++++++++++

The conclusions and pleadings in these proceedings took place in Dutch at the public hearing of 21 September 2015

Following deliberation the President of the Dutch-Speaking Court of First Instance of Brussels issues the following order:

Considering:

- the writ of summons served on 10 June 2015
- the conclusions of the plaintiff filed at the clerk of the court's office on 17 August 2015;
- the conclusions of the first defendant filed at the clerk of the court's office on 20 July and 16 September 2015
- the conclusions of the second defendant filed at the clerk of the court's office on 15 July 2015
- the conclusions on behalf of the third defendant filed at the clerk of the court's office on 20 July and 16 September 2015

* * *

1. Relevant facts and antecedents:

Facebook, Inc. is a company under the laws of the United States of America, with head office in Menlo Park, California, United States. Facebook Inc. offers the Facebook service to internet users in the United States and Canada.

Facebook Belgium SPRL is a Belgian company which was incorporated in 2001 to ensure relations with the public administration and lobbying. There were already over 4 million registered Facebook members in Belgium at that time.

Facebook Ireland is a company under Irish law. Facebook Ireland offers the Facebook service to EU users through the website www.facebook.com, in accordance with the Facebook Statement of Rights and Responsibilities.

The defendants state that Facebook, Inc. does not offer the Facebook service to Internet users in the EU, and that it does not control the personal data of EU users. According to them, Facebook Ireland is the only legal person controlling the personal data received as a result of the operation of the Facebook service outside

the United States and Canada. Thus, Facebook Ireland is said to be the sole controller for the processing of data received through the Facebook platform, including data received through cookies and plug-ins relating to the browsers on devices or equipment of Belgian Internet users. It is said that there are certain meaningful differences between the Facebook service 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.

If a certain web page is created on the Internet, website owners publish or show their own content from their own servers ("first-party" servers), but they also make content of other websites available, which is stored on "third-party" servers of those websites.

If a user wants to read a certain web page (which is also known as n http request), the browser automatically sends certain information to every "first-party" and "third-party" server on which the requested content is stored. This information typically contains the IP address for the network node used by the computer to transfer the request, the URL of the website which provided the link to the first-party website, and all cookies previously placed by the website to which the browser sends a content request (regardless of "first party" or "third party").

Subsequently the first-party server sends the information from the web page to the browser. Apart from the web page's first-party content, this information contains the instructions for the browser to load the third-party content which the website developer has selected for the website.

The Internet user's browser accepts that information without any intervention or request from third-party servers and sends an http request to the third-party servers to obtain the content needed to further load the website. These http requests typically contain (1) an IP address; (2) the URL of the first-party website; (3) the operating system of the browser; (4) the type of browser, and (5) the cookies (previously) placed by the third-party website from where the browser requests the third-party content.

The third-party websites therefore automatically receive all cookies related to the third-party website from which content is requested, as well as the IP address linked to the request and the identity of the first-party website visited by the Internet user.

A cookie is a simple text file which a web server sends to a browser requesting access to the server. The browser stores its in a folder for later use. Browser have been designed in such a way that cookies stored in a

browser are automatically communicated to the web server which initially sent them every time the browser requests access to that server, so that the server can identify which request belongs to which browser and browser-specific information can be retrieved which is needed to efficiently make the requested services and content available.

Some cookies can contain a series of (alphanumeric) characters which match with a browser (the random "identifier"). Cookies often use a machine-generated random identifier enabling the web server to make a distinction between the browsers sending requests to log and count "unique" browser requests (these are the logged server 'hits' (visits) of unique, non-overlapping browsers during a certain period of time, for instance). Every time the machine sends another request to the web server, the cookie will be scanned and the web server will be able to log the random identifier contained in the cookie, and thus continue to work with the information which was already communicated earlier during the logged session.

Cookies can also enable websites to offer a time-saving "remember me" function to registered users, which is based on cookies enabling a spontaneous login whenever a user opens the website. Consequently, it is not necessary to always re-enter this information when a page on the website is visited by a specific browser or device, and this makes it possible for users to increase the security of their account by using more complex passwords and password sentences.

More particularly, website owners use cookies to ensure the security of the personal data of their registered users, prevent malicious hacking, and avert spam attacks. Cookies notably help warn a website when some tries to log in to an account from a new location and help websites to identify spam, denial-of-service attacks or other malicious activities.

A plug-in is a piece of so-called content (or software) which website owners can integrate into their web pages for visitors to benefit from a functionality or content offered by a third-party website. It is website owners who decide which plug-ins are integrated into their websites and to what extent.

A website owner adds a plug-in on a website by embedding an instruction in the website which orders the visitor's browser to send an http request to the servers of the enterprise offering the plug-in feature. This feature is then uploaded to the visitor's browser directly from this enterprise's server. Plug-ins thus enable website owners to

drastically increase the offer of advanced functionalities and content on their websites.

Social plug-ins are a type of plug-in enabling websites to let their visitors, among others, share content with their social network by, for example, posting a reaction or a comment on an article through a Facebook plug-in, to enrich a discussion or to "like" an article and share this with the user's social media contacts or draw their attention to this. Website owners can thus use existing user communities through social plug-ins, without having to develop their own features.

Like many other online enterprises, the Facebook service offers a range of social plug-ins which website owners can choose to integrate into their websites. These functionalities enable holders of a Facebook account to share information in a simple way, and to communicated about it with other users of the Facebook service with whom they have chosen to share content (their so-called "Facebook friends") while surfing on non-Facebook websites.

For instance, the "like" button enables website owners to place this button on their websites so that visitors can indicate in respect of their Facebook friends and the other persons visiting this website that they approve of this content ("like it"). Internet users (including non-registered Facebook users) can thus see the number of "likes" given to a web page.

Other Facebook plug-ins, such as the Facebook "react" plug-in, enable website owners to show the reactions and comments of holders of a Facebook account directly on their pages, which obviously strongly simplifies communication and interaction.

Furthermore, Facebook Ireland keeps access logs which log information about devices or browsers whenever a request is sent to the servers of the Facebook platform in order to load a facebook.com web page or a social plug-in of a Facebook service. It states that it does this to guarantee the security of the Facebook service and to improve the latter's services.

This information also includes data about whether the datr cookie is present in the browser. As Facebook Ireland states, these access logs achieve and serve essential objectives of website integrity, efficient and – especially – security for Facebook Ireland.

It also states that it only keeps a record of this data for a period of time which is long enough to actually ensure security, and that it only stores the log data relating to the browsers of Internet users who do not have a Facebook account for a period of ten days after their creation.

The data included in the access logs of Facebook Ireland's web servers contains anonymous IP address details and anonymous datr browser cookie identifiers (so-called 'browser identifiers'). According to Facebook Ireland it would not be possible for a website operator to identify or single out an individual non-registered user based on this information alone.

Facebook Ireland states that it only places the datr cookie if an Internet user with a Facebook account or a non-registered user of Facebook (i.e. a person choosing to visit a website of the facebook.com domain or to interact with a Facebook plug-in on a third-party website), explicitly interacts with the Facebook service.

It states that it does not apply the datr-cookie in the capacity of third party. Thus an Internet browser only receives the datr cookie if an Internet user directly interacts with the Facebook service, like (i) when visiting a page on facebook.com, or (ii) actively interacting with Facebook content such as a social plug-in.

The debates have shown that since the summons was issued in this case, Facebook has deployed a cookie banner throughout the EU, including Belgium, for non-registered users of Facebook to meet conceivable concerns, if any, relating to the adequate nature of consent. The cookie banner was designed based on the discussions started with the Irish DPC last year and according to Facebook Ireland it is deployed in the EU to enhance the consent granted by EU Internet users when they interact with the Facebook service.

During a first visit to a facebook.com website, Facebook shows a "cookie banner" explaining that Facebook uses cookies if a visitor of the Facebook platform is a non-registered user. Facebook Ireland also provides a link to additional information about how the Facebook platform uses cookies.

The defendants now state that if the user leaves the page or follows the link to learn more information about the cookie, no cookie is placed.

The Privacy Commission claims the contrary.

Moreover, it is said that there is a cookie link on virtually every facebook.com page, and the information communicated by Facebook Ireland in its cookie policy explains that in these situations cookies are used for the security of the website and the user.

According to Facebook Ireland it obtains consent through this banner prior to placing the datr cookie.

Facebook Ireland states that the datr security cookie plays a most crucial role in the protection of the Facebook service against a whole series of security threats, to the benefit of both users with a Facebook account and non-registered Facebook users, and in its conclusions it gives approximately ten examples in this context.

Facebook Ireland also states that its practices relating to the datr cookie and social plug-ins as regards non-registered users of Facebook have not changed since the extensive audit and the investigation of the Irish DPC in 2011, 2012 and 2014, nor have they changed since the entry into force of the Revised Data Policy ("revised conditions and policy rules relating to data") of 30 January 2015. When drawing up this audit, the Irish DPC cooperated and consulted with other European supervisory authorities for data protection, including the Article 29 Working Party which organises consultation between the European supervisory authorities, including the Belgian Privacy Commission.

Following the announcement in November 2014 of the modification of the terms of use and queries in this regard from worried Facebook users, the media, the federal parliament and the Secretary of State for Privacy, the Privacy Commission started a technical and legal investigation in order to examine the compatibility of these new terms of use and the modifications with the Belgian privacy legislation. To do so it appealed to the technical expertise of scientific researchers of the *Katholieke Universiteit Leuven* and the *Vrije Universiteit Brussel,* who had already conducted extensive research into Facebook in the context of their ongoing research projects.

On 31 March 2015 they published the most recent version of the research report "From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms" on the website of the Interdisciplinary Centre for Law and ICT (ICRI) of the KU Leuven.

One of the findings of the research report is that Facebook also processes personal data of Internet users who do not have a Facebook account,

through social plug-ins and cookies which Facebook uses to register the websites visited by persons not having a Facebook account.

Social plug-ins are extremely popular among website owners, since their website attracts more visitors when visitors inform their "friends" that they like that website by clicking on the social plug-in button. The "Like" button (Facebook's most popular social plug-in) is present on no less than 32% of the 10,000 most visited websites from all possible categories of websites.

The research report shows that whenever someone who is not a Facebook user visits a website of the facebook.com domain, including the personal Facebook pages of persons and companies or other organisations, Facebook automatically places a cookie on that visitor's hard disk. Such web pages, which are all accessible in Belgium, are also visited by non-users of Facebook from Belgium.

The relevant cookie, called "datr" cookie by Facebook which has already been mentioned above, contains information uniquely identifying an Internet user's browser and remains on his hard disk for two years.

When that Internet user subsequently visits a website with a social plug-in button of Facebook, then as a rule his browser will automatically connect to the Facebook server to collect the plug-in. As a result of this connection, information from Facebook's datr cookie, which was stored on the user's hard disk, is sent to the Facebook servers.

Following this investigation extensive correspondence took place between the Privacy Commission and Facebook.

In that correspondence Facebook stated, among others, that Facebook Ireland Limited should be considered as the controller and that is was prepared to provide an oral explanation about its services but it denied the applicability of Belgian privacy law and the competence of the Belgian Privacy Commission, advising that if the Belgian Privacy Commission has concerns about the processing of personal data in Belgium by Facebook, it has to contact the Irish privacy commission, which according to Facebook is the only competent authority for Facebook's activities in the EU.

In its letter of 6 March 2016 Facebook also confirmed that it does not use sensitive data for personalised advertisements.

After a first meeting on 15 April 2015, the Privacy Commission heard Facebook representatives in the context of a recommendation procedure during a hearing on 29 April 2015.

On 13 May 2015 the Privacy Commission issued a Recommendation based on Article 30 § 1 of the Privacy Act, with a legal analysis of the technical findings in the research report relating to the social plug-ins and cookies of Facebook.

In its Recommendation the Privacy Commission states, among others, that Belgian privacy legislation applies and that the Privacy Commission has jurisdiction for law enforcement regarding the recording by Facebook of the surfing behaviour of Internet users from Belgium. It also stated, among others, that the processing by Facebook of personal data of Internet users who do not have a Facebook account by means of cookies and social plug-ins, such as the collection of data relating to which websites are visited by Internet users from Belgium who do not have a Facebook account, constitutes a violation of the Privacy Act and of Article 129 of the Act on electronic communication (ECA).

Relating to non-users of Facebook the Privacy Commission ordered that Facebook must refrain from systematically placing long-life and unique identifier cookies with non-users of Facebook.

By registered letter and e-mail of 18 May 2015 the Privacy Commission served notice of default on Facebook Inc. and Facebook Belgium SPRL for their violations of the Privacy Act and Article 129 of the ECA, and it urged them to advise on 27 May 2015 at the latest whether they intended to end those violations.

By registered letter an e-mail of their counsel of 26 May 2015 Facebook Inc. and Facebook Belgium SPRL replied that they wished to consult with the Privacy Commission on the recommendation and they requested an appointment for a discussion.

The subsequent exchange of e-mails and letters, however, did not bring them closer to each other, since the Privacy Commission maintained its position that it has jurisdiction and that Belgian legislation applies, and the Facebook must immediately end the processing of personal data of non-users of Facebook. The defendants on their part basically continue to state that at least implicitly, if not explicitly, they have users' consent to this processing, and that only the Irish privacy commission is competent for its activities in the EU. Basically Facebook even states that the Belgian Privacy Commission's claim for Facebook to acknowledge its competence and the applicability of Belgian law, constitutes a refusal to start a constructive dialogue.

Considering that the Privacy Commission assumes that Facebook will not end this contested processing, it initiated the present summary proceedings in the person of its president.

2. Claims of the parties.

Currently Mr WILLEM DEBEUCKELAERE, acting in his capacity of PRESIDENT OF THE BELGIAN COMMISSION FOR THE PROTECTION OF PRIVACY, requests the president of the Dutch-language Court of First Instance of Brussels, sitting in summary proceedings, to declare the claim admissible and substantiated.

Accordingly, to sentence Facebook Inc., Facebook Belgium SPRL and – if it is held that Facebook Ireland Limited is the controller of the processing operations of personal data in Belgium or is in any other way involved therein (*quod non*) – order Facebook Ireland Limited, by way of a temporary measure in respect of every Internet user on Belgian territory who has not registered as a member of the social network of Facebook, to cease:

- placing a datr cookie when they land on a web page of the facebook.com domain without providing them with prior sufficient and adequate information about the fact that Facebook places the datr cookie with them and about Facebook's use of that datr cookie through social plug-ins;
- collecting the datr cookie placed on third-party websites through social plug-ins.

All this under penalty of a fine, jointly and severally, at least the one in the absence of the other, of EUR 250,000 per day for every day there is a violation starting from the date of the decision to be pronounced;

To sentence the defendants to the costs of the proceedings, including the cost for the service of the writ of summons and the compensation towards the administration of justice, the latter at present estimated at 1,320 euros for each defendant;

Declare the decision to be pronounced immediately enforceable, notwithstanding any legal remedy and without any security and excluding the right to apply for a restriction of security.

The company under the law of the State of Delaware FACEBOOK, INC on the other hand requests the president of the court:

-- to declare himself without jurisdiction
-- in a subordinate manner, to declare the claim impermissible and at least inadmissible;
-- in an even more subordinate manner, to dismiss the claim as unsubstantiated; and

-- in all cases to sentence the Plaintiff to the costs, estimated for the first defendant at 1,320 euros by way of compensation for the administration of justice.

Furthermore FACEBOOK BELGIUM SPRL requests the president
-- to declare himself without jurisdiction;
-- in a subordinate manner, to declare the claim impermissible and at least inadmissible; and
-- in an even more subordinate manner, to dismiss the claim as unsubstantiated,
-- in an entirely subordinate manner, not to pronounce the prohibition in respect of the second Defendant Facebook Belgium.
-- in all cases to sentence the Plaintiff to the costs, estimated for FACEBOOK BELGIUM SPRL at € 1,320 by way of compensation for the administration of justice.

Finally the company under Irish law FACEBOOK IRELAND LIMITED requests the president of the court
-- to declare himself without jurisdiction;
-- in a subordinate manner, to declare the claim impermissible and at least inadmissible;
-- in an even more subordinate manner, to dismiss the claim as unsubstantiated; and
-- in all cases to sentence the Plaintiff to the costs, estimated for the third defendant at € 1,320 by way of compensation for the administration of justice.

3. Evaluation

3.1. International Jurisdiction and Applicable Law:

Article 4 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data stipulates:

"*Article 4*

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself."

In this case the Privacy Commission, through its president, also summoned FACEBOOK BELGIUM SPRL. The defendants do not contest that FACEBOOK BELGIUM, as a daughter company of FACEBOOK GLOBAL HOLDINGS LLC and FACEBOOK GLOBAL HOLDINGS II LLC, is a part of the FACEBOOK Group in which the first defendant FACEBOOK INC is the parent company and has the lead.

FACEBOOK BELGIUM SPRL, established in Brussels, is a Belgian establishment of the controller of the processing of the data on the Facebook network. The court agrees with the Privacy Commission where it states that eventually, for the application of Article 4.1.a) of Directive 95/46/EC, it is of no importance in this case whether the controller is FACEBOOK INC. or FACEBOOK ITELAND LIMITED: it cannot be denied that FACEBOOK IRELAND LIMITED, through FACEBOOK CAYMAN HOLDINGS UNLIMITED IV and FACEBOOK IRELAND HOLDINGS, is also a part of the FACEBOOK Group.

Moreover, it is of no importance whether the processing takes place on the territory of an EU Member State or outside the EU. The application of Article 4.1.a) of Directive 95/46/EC does not depend on that. In this regard it must first of all be observed that point 19 of the preambles of Directive 95/46 specifies that "*establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements*" and "*the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect*".

The defendants state themselves that Facebook Belgium SPRL is a Belgian company which was incorporated in 2011 in order to ensure relations with the public administration and lobbying.

Moreover, the conclusion of Facebook Belgium SPRL of 15 July 2015 and the conclusion of 20 July 2015 of Facebook Inc. show that two members of staff of Facebook Belgium are in contact with Belgian enterprises to provide support services relating to the marketing and sale of advertising space by Facebook Ireland, and that two of its employees provide support to Facebook Ireland when it comes to advertising.

With quotes from the most recent financial statement of Facebook Belgium and the hearing of 29 April 2015 the Privacy Commission convincingly demonstrates that the company's main activity in 2014 consisted of public policy support, sales support and the provision of marketing services to the Facebook Group.

This means that the activities of the controller and those of Facebook Belgium SPRL are inextricably linked in the meaning used by the Court of Justice of the EU in judgement C-131/12 of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling from the Audiencia Nacional — Spain) – Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja Gonzalez (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131):

"52 Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.

53 Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C‑324/09 L'Oréal and Others EU:C:2011:474, paragraphs 62 and 63).

54 It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

55 In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State,

advertising space offered by the search engine which serves to make the service offered by that engine profitable.

56 In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

57 As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory."

Taking into account this objective of Directive 95/46 and the wording of its Article 4, paragraph 1, a, it must be considered that the processing of personal data to the benefit of a service of a social network site such as Facebook, which is operated by an enterprise with its Registered Office in a third country but an establishment in a member state, is carried out "*in the context of the activities*" of this establishment if the establishment is intended to ensure the promotion and sale in that member state of advertising space offered by this social network site, which is intended to make the service offered by this social network profitable.

In this context it must be reminded that simply showing personal data on a Facebook page constitutes a processing of such data. Since showing this Facebook page involves showing, on the same web page, advertisements related to the activities of the user, it must be established that the concerned processing of personal data is carried out in the context of the advertising and commercial activity of the establishment of the controller on the territory of a member state, in this case Belgian territory.

Incidentally, the court is of the opinion that ensuring relations with the public administration and lobbying activities by this establishment are also an activity which is intended to make the service offered by this social network profitable, so that the activities of Facebook Belgium are therefore inextricably linked to activities of the operator of the social network site.

That Facebook Belgium itself does not process the personal data or that it is said not to conclude contract with advertisers, is irrelevant. The determining factor for the application of Article 4.1.a) of Directive 95/46/EC is not based on that, but on the finding that the activities of Facebook Belgium are therefore also inextricably linked to the activities of the operator of the social network site.

The above means that Belgium in this case, based on Article 4.1.a) of Directive 95/46/EC, can apply its national provisions implementing this directive to the processing of personal data since it is carried out in the context of the activities of an establishment on Belgian territory of the controller. Considering that the same controller has an establishment on the territory of several Member States, he must take the necessary measures to ensure that each of those establishments, including the Belgian one, meets the obligations imposed by applicable national legislation, in this case Belgian legislation.

Consequently, the Privacy Commission did not use Facebook Belgium's presence artificially in these proceedings and the multiple summons cannot be compared with 'Belgian Torpedo' – now defunct – with which some people intended to sabotage the jurisdiction of foreign courts in the past: the present case is about the application of Belgian legislation on Belgian territory and Facebook Belgium is indeed a Belgian establishment of the controller of the processing of the data in the meaning of Article 4.1.a) of Directive 95/46/EC.

The Belgian judge thus has international jurisdiction to decide on the present claim, and furthermore he applies Belgian legislation in the process.

This is all the more true because the president of the Court of First Instance sitting in summary proceedings has full jurisdiction. Even if only a foreign judge had jurisdiction for the case on the merits, then still the Belgian civil-law judge in summary proceedings would have jurisdiction (see, among others, J. LAENENS, K. BROECKX, D. SCHEERS and P. THIRIAR, *Handboek Gerechtelijk Recht*, Antwerp, 2012, Intersentia, p 263, no. 596) to take temporary measures.

3.2 Competence

When investigating whether the judge in summary proceedings is competent, he must verify whether the document instituting the proceedings shows urgency explicitly, or even implicitly.

The writ of summons mentions that the case is urgent. The judge in summary proceedings is therefore competent to investigate on the merits. (Cass., 11 May 1990, Pas., 1990, I, 1045).

3.3 Admissibility of the claim

Facebook, Inc. understands that the writ of summons was sent both by letter and through the Central Authority. Since Facebook, Inc. can confirm that it received the writ of summons through the Central Authority on 20 August 2015, it no longer discusses the matter of the absence of service since this no longer serves any useful purpose.

In turn, however, the court cannot discuss the allegedly illegitimate shortening of the term to issue the summons since this would violate the authority of the final nature of the decision of 5 June 2015 of the vice-president of this court, who was designated to replace the president and who authorised the shortening of the terms to issue the summons. The present proceedings do not constitute third-party proceedings nor an appeal against this decision and cannot be considered as a legal remedy against it. The consideration in this decision that it does not bind the judge in summary proceedings in his evaluation of the urgency, only applies to the urgency of the summary proceedings, but this does not prevent that the shortening of the terms to issue the summons is authorised by a judicial decision having a final nature.

Article 32 § 3 of the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data stipulates:
"Art. 32. (…)
§ 3. Without prejudice to the competence of regular courts and tribunals regarding the application of the general principles concerning the protection of privacy, the President of the Commission may submit any dispute relating to the application of this Act and its corresponding measures to the Court of First Instance."

This immediately establishes that the President of the Commission for the Protection of Privacy has an interest and the capacity to bring the present claim. Where the court uses "the Privacy Commission" further on in this decision, instead of "the President of the Commission for the Protection of Privacy", this is the result of the fact that the president naturally does not exercise his competence in his own name, but in his function as president and representative of the Privacy Commission.

The Act of 13 June 2005 on electronic communication constitutes the transposition into Belgian law of (among others) 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. EU 31 July 2002, L 201/37 (Art. 1 of the Act). In its Article 1 this Directive stipulates:
"*Article 1*

Scope and aim

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons. (…) "

Now that the Act of 13 June 2005 on electronic communication constitutes a transposition of this directive, it also contains a specification and a complement of Directive 95/46/EC of which the Privacy Act is a transposition.

As such – and only as such – the Privacy Commission can invoke Article 129 of the ECA. Also Article 129 of the ECA which the Privacy Commission invokes, even contains a twofold reference to the Privacy Act, where it states that the concerned subscriber or user, pursuant to the conditions laid down in the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, must be given clear and precise information about the purposes of the processing and his rights based on the Act of 8 December 1992, and that this consent does not exempt the controller from the obligations of the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data which are not imposed in the Article.

3.4 Urgency

There is urgency in the meaning of Article 584, first paragraph of the Judicial Code when the fear of damage of a certain scope, or of serious inconvenience makes it necessary to take an immediate decision (Cass. 21 May 1987, Pas., 1987, I, 1160).

The plaintiff makes it plausible that the claim is urgent since a claim relating to basic rights and freedoms (fundamental rights) which have been violated by an action of the defendant, is always urgent.

Several preambles, among others especially preamble 10 of Directive 95/46/EC, show that this explicitly aims at the protection of fundamental rights:
"*(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;*"

Moreover, the Privacy Commission justly indicates that the alleged violation does not only relate to the fundamental right of one person, but of an enormous group of persons, because there are an uncountable number of Internet users in Belgium who do not have a Facebook account and who have already ended up on a web page of the facebook.com domain, and on whose computer Facebook's datr cookie would consequently be placed without their knowledge. Because of the millions of websites with Facebook's social plug-ins it is almost impossible to escape this. This also relates to very sensitive information which shows e.g. health or religious, sexual or political preferences (e.g. people who visit numerous websites regarding a health problem or a religious, sexual or political preference).

An immediate decision to prevent this massive number of alleged violations would thus be desirable. The claim is urgent.

The Belgian Privacy Commission has also not been negligent, because it took action immediately after the abovementioned "Google Spain" judgement was pronounced, which implied a fundamental modification of the case law on the competence of EU member states in respect of Internet companies which operate on their territory without processing personal data locally, but do have an establishment there. The investigation the Privacy Commission conducted and had conducted into the alleged violations and subsequent discussions with Facebook naturally took a lot of time, so that the Privacy Commission cannot be blamed for having been slow in issuing the summons and consequently having created the urgency itself.

3.5 Investigation into the way of summary proceedings:

Apparently Facebook places the datr cookie when an Internet user visits a web page of the facebook.com domain, regardless of whether he is a Facebook user or not. This cookie has a life of two years. During these two years,

the cookie stays on the Internet user's computer, unless the Internet user deletes it himself.

If this Internet user then visits a website with a social plug-in of Facebook, when loading the content of the social plug-in the Facebook server will request that the browser of the data subject transfers the datr cookie. The datr cookie, however, is not the only part of the communication between the browser and the Facebook server: the Internet user's IP address and the URL of the website the plug-in is on are also transferred. Transferring the IP address in particular is an essential property of TCP/IP, the protocol which enables communication through the Internet and which HTTP uses to build on.

Because of the combination of the datr cookies, the IP address and the website visited by the Internet user, Facebook is able to monitor the surfing behaviour of the individual Internet user.

The present claim by the Privacy Commission aims at hearing the declaration that Facebook, because it (a) places the datr cookie on the computers of Belgian non-users of Facebook and because it (b) then requests the information from this cookie whenever Belgian non-users of Facebook visit a website on which a social plug-in of Facebook has been integrated, violates the Privacy Act as well as Article 129 of the ECA.

According to the Privacy Commission Facebook thus violates Articles 4 and 5 of the Privacy Act: "*Art 4. § 1. Personal data must be:*

1° processed fairly and lawfully;
2° collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions and must not be further processed in a way incompatible with those purposes. Under the conditions established by the King, having received the opinion of the Commission for the Protection of Privacy, further processing of data for historical, statistical or scientific purposes is not considered incompatible;
3° adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;
4° accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that data which is inaccurate or incomplete with respect to the purposes for which it is collected or for which it is further processed, is erased or rectified;
5° kept in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed. Having received the opinion of the Commission for the Protection of Privacy, the King shall establish appropriate

safeguards for personal data stored longer than stated above for historical, statistical or scientific purposes.
§2. The controller must ensure compliance with § 1.

Art 5. Personal data may only be processed in the following cases:
a) the data subject has unambiguously given his consent;
b) the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c) the processing is necessary for compliance with an obligation to which the controller is subject under or by virtue of an act, decree or ordinance;
d) the processing is necessary in order to protect the vital interests of the data subject;
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller or in a third party to whom the data is disclosed;
f) if the processing is necessary for the promotion of the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act.

By decree after deliberation in the Council of Ministers, having received the opinion of the Commission for the Protection of Privacy, the King can specify the circumstances in which the condition stipulated under f) is considered as not having been met."

Furthermore, according to the Privacy Commission Facebook violates the rights of the data subjects by not providing them with prior information although this is prescribed by Article 9 of the Privacy Act.

Finally, according to the Privacy Commission Facebook violates Article 129 of the ECA by systematically, without having obtained the prior, freely given, informed an unambiguous consent of non-users of Facebook, collecting the datr cookie every time when the non-user of Facebook visits a third-party website with a Facebook social plug-in.

The court cannot agree with Facebook's argument that the information it collects would only enable the identification of a computer and that this data is not personal data.

Articles 2 of Directive 95/46/EG and 1 §§ 1 and 2 of the Privacy Act define the concepts of "personal data" and "processing of personal data" as follows:
"Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;"

The datr cookie which Facebook places on the computer of an Internet user and by means of which it receives information, uniquely identifies the Internet browser of an Internet user. The cookie contains a "unique identifier". Facebook also receives additional information enabling it to directly or indirectly identify individuals, such as the IP address of the Internet user's computer.

Both the Court of Justice of the EU and the "Article 29" Data Protection Working Party have already confirmed explicitly that IP addresses are "personal data" (see among others Court of Justice *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* of 24 November 2011 C-70/10, marginal no. 51 *i.f. "Those addresses are protected personal data because they allow those users to be precisely identified."*).

Since the defendants state themselves that the datr cookie is used, among others to perform a certain type of access control and therefore partially to determine who will be granted or denied access to a Facebook service, the datr cookie as such must also be considered as personal data.

The automated processing of IP addresses and uniquely identifying

browser cookies such as the datr cookie is consequently a processing of personal data, because this perfectly matches the definition of Article 2 of Directive 95/46/EC and Article 1 § 2 of the Privacy Act.

This processing, including the simple storage or the simple automated reception of this data from the browser of a user visiting a website with a "Social Plug-In", must therefore meet the conditions of Articles 4 and 5 of the Privacy Act. Whether Facebook stores the data for a long or only a short period, is therefore irrelevant.

In case of a user who is on Belgian territory but has never registered on Facebook, nor granted valid consent in any way with Facebook's terms of use, but who did land on the facebook.com domain, which resulted in the placing of a datr cookie, the defendants do not demonstrate that they were authorised place this datr cookie and later receive it again based on any unambiguous authorisation of the user (Art. 5.a. of the Privacy Act).

Relating to the storage of information or obtaining access to information already stored in the end user's final equipment, which is what placing cookies and reading them again manifestly is, Article 129 of the ECA very clearly stipulates:
"Art. 129. Storing or obtaining access to information which has already been stored in the final equipment of a subscriber or a user is only authorised provided that:
1° the subscriber or user concerned, pursuant to the conditions laid down in the Act of 8 December 1992 on the protection of personal data in relation to the processing of personal data, is given clear and precise information about the purposes of the processing and his rights based on the Act of 8 December 1992;
2° the subscriber or end user has granted consent after having been informed pursuant to the stipulations in 1°.
The first paragraph shall not apply to the technical storage of information or access to information stored in the final equipment of a subscriber or and end user with the exclusive purpose of sending a communication through an electronic communication network or providing a service explicitly requested by the subscriber or end user, when this is strictly necessary for this purpose.
Consent in the meaning of the first paragraph or the application of the second paragraph does not exempt the controller from the obligations of the Act of 8 December 1992 on the protection of personal data in relation to the processing of personal data which are not imposed in this Article.
The controller shall offer subscribers or end users the possibility to revoke consent free of charge and in a simple way."

In this regard the Irish privacy commission has stated:

"Not all cookies require consent to be used. These are cookies essential to delivering the service requested by the user – session cookies, authentication cookies (for the duration of the session,) and user security cookies. For example, for storage of items in a shopping cart on an online website advance consent will not be required. This will generally be the case where the cookie is stored only for as long as the "session" is live and will be deleted at the end of the session."

The contested datr cookie, which does not disappear when ending the session, but remains stored in the folders used by the browser for another two years, does not meet this description, however, and it is seemingly subject to the rules of Articles 4 and 5 of the Privacy Act and 129 of the ECA.

At the hearing there was much ado about the banner which Facebook has recently placed in its homepage and which apparently is always shown to a user who has never visited a page of the facebook.com domain before, and which reads:
"Cookies help us provide, protect and improve Facebook's services. By continuing to use our site, you agree to our cookie policy."

By clicking on the hyperlink behind the words *"our cookie policy"* visitors are brought to a page *"Cookies, Pixels and Similar Technologies",* which provides quite some explanation about cookies, although the datr cookie as such is not mentioned there.

Apparently the datr cookie is not placed at that moment yet, but it is placed in case of further clicks of the non-registered user on this page, for instance on the hyperlinks "*Facebook services"* or "*our Statement of Rights and Responsibilities".*

Likewise the datr cookie is apparently not placed when a non-registered user, clicks on a Facebook social plug in, consciously or not, from a web page outside the Facebook domain. But if the user then clicks "cancel" to close the social plug-in, apparently the cookie is indeed placed.

The court is of the opinion that Facebook cannot consider these actions as granting informed consent, because in the first case the user is still gathering information, and further examining the information cannot be considered as use of the Facebook services. In the second case the same non-registered user, precisely by closing the social plug-in, indicates that he does not wish to use the service offered.

Likewise the court is of the opinion that Facebook does not have informed and unambiguous consent to read a previously placed datr cookie from a non-registered user's browser. After all, pursuant to Article 129 of the ECA the controller must have consent to store information as well as gain access to information which is already stored in a user's final equipment.

Moreover, a non-user of Facebook who once visited the facebook.com domain (and consequently had Facebook's datr cookie place on his hard disk) cannot be qualified as a "user" in the meaning of Article 129 of the ECA, who explicitly requests a Facebook service every time he visits a third-party website on which as social plug-in has been implemented.

In the opinion of the court persons who do not have their own Facebook account but who once visited a page of the Facebook domain, cannot be considered as "users" of Facebook's services, be it only because visitors can also land on the Facebook page of a person or an organisation without wanting this at all, for example by following a link from a web page outside the Facebook domain without knowing that this link will take them to a Facebook page.

The court agrees with the Privacy Commission where it states that it has not been demonstrated that people who once visit a web page of the facebook.com domain, allegedly consented to Facebook's terms of use, a link to which is nowhere on that page, and therefore allegedly granted consent to have the datr cookie placed on their hard disk. In this case a distinction can only be made between Internet users who have a Facebook account and those who do not have a Facebook account but do once visit a web page of the facebook.com domain. For the former it can be assumed that they at least implicitly but unambiguously consented to placing and later on reading the datr cookie, but for the latter the defendants must demonstrate this, and it has already been elaborated above that this has not been demonstrated.

Since the personal data of non-registered users, especially in case of ill-considered use of the banner or of the social plug-in, can already be processed before this non-registered user is able to obtain complete information or does 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 or it is further processed in a way which, taking into account all relevant factors, i.e. the reasonable expectations of the data subject and the applicable statutory and regulatory provisions, is incompatible with those purposes.

This is a seeming violation of Article 4, 1° and 2° of the Privacy Act.

Finally it holds true that the first-party role which Facebook possibly plays when placing the datr cookie is not maintained if it collects the cookie at a later time through social plug-ins implemented on websites outside the Facebook domain, and therefore acts as a third-party in the Internet use of the non-registered user. As the third-party, at that time it only has a connection with the owner or creator of the website visited, but not with the visitor of that page who does not explicitly use the services of this third party.

Also the alleged extension of the already deficient consent of the non-registered user, apparently leads to an unfair and unlawful processing of personal data which does not take into account the reasonable expectations of the non-registered user, which appears to be a further violation of Article 4,1° and 2° of the Privacy Act.

Now that it is clear that the defendants can seemingly not invoke the informed and unambiguous consent of non-registered visitors for the contested processing, it must be investigated whether they can invoke the other grounds for authorisation of Article 5 of the Privacy Act.

Now that the defendants do not have an agreement with a user who is on Belgian territory but who has never registered on Facebook, nor has granted valid consent to Facebook's terms of use in any way, they cannot invoke any necessity of the contested processing to perform a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.

Based on Article 16 § 4 of the Privacy Act the controller and his representative in Belgium, if any, as well as the processor, in order to safeguard the security of the personal data, must take the appropriate technical and organizational measures that are necessary to protect the personal data from accidental or unauthorized destruction, accidental loss, as well as from alteration, access and any other unauthorized processing of the personal data. These measures must ensure an appropriate level of security taking into account the state of technological development in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other.
Having received the opinion of the Commission for the Protection of Privacy the King may issue appropriate standards relating to information security for all or certain categories of processing.

This does not mean, however, that for the defendants the contested processing of personal data is necessary to meet an obligation the controller is subject to by virtue of or under an act, a decree or an ordinance.

It must first of all be verified whether a ground for authorisation from Article 5 can be invoked, if not the personal data must not even be processed. It is only when the personal data may be processed, that the obligation arises to take the appropriate technical and organizational measures that are necessary to protect the personal data from accidental or unauthorized destruction, accidental loss, as well as from alteration, access and any other unauthorized processing of the personal data.

Having a ground for authorisation is a basic obligation which does not depend on the other obligations from the Privacy Act. Legal obligations in the meaning of Article 5.c of the Privacy Act are therefore obviously only obligations which are in other acts than the Privacy Act itself, for instance obligations from labour and social security legislation.

Judging this otherwise would lead to circular reasoning, as a result of which any type of personal data may always be processed, which would lead to erosion of the entire Act on the protection of privacy in relation to the processing of personal data.

Since the integrity of stored or processed data must always be safeguarded, one could consequently always invoke that the processing is authorised, and one would thus never have to refrain from processing personal data.

This would create a completely absurd situation in which Facebook users have to grant explicit consent to the processing of their personal data, and non-users of Facebook – without having granted any consent – would have to tolerate that their personal data are also processed to secure the personal data of others. This is obviously impossible: every data subject must be able to consent to the processing of his personal data himself.

In this situation it holds true that the measures taken must not go against the quality requirements included in Article 4 of the Privacy Act, which would mean that they lack any appropriate nature. Considering the entirely excessive nature of the contested processing operations, there is no "appropriateness" of the measures taken. Consequently, Article 16, §4 of the Privacy Act cannot be used as a ground for legitimacy at all.

Furthermore, it cannot be understood why the contested processing is necessary to safeguard a vital interest of non-registered users.

The defendants furthermore do not demonstrate and do not even invoke that they were instructed to perform a task carried out in the public interest or in the exercise of official authority.

The sixth and final ground for authorisation is the necessity of the contested processing to promote the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act.
By decree after deliberation in the Council of Ministers, having received the opinion of the Commission for the Protection of Privacy, the King can specify the circumstances in which the condition stipulated under f) is considered as not having been met.

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.

The defendants state that the datr cookie helps in case of attacks targeting the Facebook platform, essentially in case of attempted fraudulent access. It can be assumed that this is true to a certain extent when contact is made with a Facebook page, but in the situation at hand, non-users of Facebook do not wish to connect with the Facebook-platform but only to visit an entirely different website. The defendants do not make it plausible that an attack of the Facebook platform would be possible through plug-ins which are not actually used by users who access a page outside the Facebook domain.

Even a "digital illiterate" understands that the systematic collection of the datr cookie alone is insufficient to counter the attacks Facebook mentions, because criminals can very easily circumvent the placing of this cookie with cookie blocker software. For a potential attacker having the necessary knowledge of IT, it must be child's play to simply block or remove cookies before or during the launch of the attack. The contested processing thus lacks the necessary efficiency to achieve the alleged security since it is sufficient for a single malicious attacker to know how cookies can be blocked in order to breach this security, this knowledge being readily available on the web and on help pages.

Moreover, there appear to be less intrusive methods to achieve the envisaged security. It is not credible, for example, that a so-called DDoS attack, which is carried out through thousands or tens of thousands of computers all over the world, each of which contains a different cookie with a "unique identifier" – or do not contain it if the code used blocks or removes it – could only be prevented by collecting the different datr cookies on the infected systems. An IT giant like Facebook most certainly has better security methods for this, so that the contested processing does not pass the test of proportionality either.

Collecting the personal data of non-users of Facebook through social plug-ins undeniably makes it possible to expose and record a significant part of the surfing behaviour of non-users of Facebook, taking into account the large number of websites with a Facebook social plug-in. Consequently, this has a serious impact on the fundamental right to privacy and the protection of personal data, and it must also be observed, moreover, that Facebook, as a large Internet group, is in a much stronger position than the individual non-user of Facebook.

The provisional weighing of the interest of Facebook against the fundamental rights of the affected non-users of Facebook undeniably tends to be to the benefit of non-users of Facebook, because the contested processing operations are clearly disproportionate considering the indicated purpose and the scale on which the processing operations are carried out and the fact that these are not fair or legitimate processing operations either.

This seemingly constitutes a violation of Article 4, 2° and 3° of the Privacy Act, according to which personal data must be obtained for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions and must not be further processed in a way incompatible with those purposes. Personal data must also be adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed.

3.6 The measure claimed:

Article 39, 1° and 2° of the Privacy Act stipulates penalties for the controller, his representative in Belgium, his agent or assignee processing personal data in violation of the conditions imposed by Article 4 § 1 and for the controller, his representative in Belgium, agent or assignee processing personal data in cases other than those in Article 5.

The obligations imposed by Article 4 § 1 and 5 of the Privacy Act thus touch upon Belgian public order, so that the claim of the President of the Commission for the Protection of Privacy does not violate the proportionality principle and the principle of non-discrimination, and there is no reason for a weighing of interests either.

The claim does not aim at hearing a prohibition of drawing up a profile for advertising purposes but rather at obliging the defendants to meet the obligations they are subject to as a controller when collecting the datr cookie from non-users of Facebook through social plug-ins on third-party websites. This obviously includes the obligation that the defendants themselves must end the violation of the proportionality principle.

Moreover, the violations have a massive scope: they do not only relate to the violation of the fundamental right of one person, but of an enormous group of persons. There are an uncountable number of Internet users in Belgium who do not have a Facebook account but who have already landed on a web page of the facebook.com domain, and on whose computer a Facebook datr cookie was consequently placed without their knowledge. On the other hand the number of websites with Facebook social plug-ins amounts to millions, so that it is almost impossible to escape from them. Very often very sensitive information is involved, showing e.g. health, religious, sexual or political preferences.

That the defendants collect data about the surfing behaviour of millions of inhabitants of Belgium who have decided not to become a member of Facebook's social network site, regardless of what they do with the data, is a manifest violation of the privacy legislation.

Considering that the violation of Articles 4 § 1 and 5 of the Privacy Act touches upon the Belgian public order, the measure claimed is not disproportionate.

It is completely implausible that the measure could not be implemented in Belgium, and it is entirely irrelevant, moreover, that technical implementations, if any, would have to take place abroad because of the internal organisational and company structure of the Facebook Group. Incidentally, it is simple for Facebook to limit the implementation of the temporary measures to Belgian territory since it can limit implementation to Belgian IP addresses if required.

The measure claimed must not only be imposed on FACEBOOK, INC. but also on FACEBOOK IRELAND LIMITED and FACEBOOK BELGIUM SPRL. Not only it has been elaborated above that the activities of FACEBOOK BELGIUM are inextricably

linked to the activities of the operator of the social network site, but furthermore the penalties of Article 39 1° and 2° of the Privacy Act apply both to the controller and his representative in Belgium, his agent or assignee processing personal data. Since the defendants themselves argue that Facebook Ireland provides the Facebook service to EU users, this company must also observe the measure to be imposed.

In this case granting the requested measure can only be combined with imposing a fine in order to put the necessary pressure on the defendants for them to observe the measure. When establishing the height of the amount of the fine, the judge shall especially take into account the financial strength of the sentenced party and the expected resistance against the enforcement of the sentence (see among others K. WAGNER, "*Dwangsom 2003-2009" in: Vlaamse Conferentie bij de Balie te Antwerpen (ed.), Meester van het proces. Topics gerechtelijk recht*, Ghent, Larcier, 2010 (I) 7).

The circumstance that the Facebook Group mainly consists of foreign companies does not prevent either that a fine can be imposed on the defendants in Belgium.

Since the Facebook Group undeniably achieved a 12.4 billion dollar turnover and a 2.9 billion dollar profit in 2014 and it is one of the companies with the greatest financial strength in the world, the claimed fine of EUR 250,000 per day of non-compliance with the measure to be ordered, seems appropriate to be sufficiently deterrent. A reasonable term of 48 hours can be granted to the defendants to implement the measure to be ordered, assuming that they have sufficient legal staff and that they are sufficiently assisted by a team of specialised lawyers to know that while these proceedings were put in place and deliberated on they had to take at least the necessary measures to prepare this implementation.

The measures claimed appear to be substantiated to the extent that has been stipulated in the body of this order and can therefore be ordered as provided for below.

3.7 Enforceability:

The court recalls that this decision shall be immediately enforceable by operation of law and without any security (Art. 1039 of the Judicial Code).

FOR THESE REASONS:

Mr W. Thiery, judge, appointed to replace the president of the Dutch-language Court of First Instance in session in Brussels, assisted by Mrs C. KINT, clerk of the court;

Considering the Act of 15 June 1935 on the use of language in legal proceedings;

Administering justice relating to the temporary measures, after having heard all the parties;

Rejecting all other or conflictual decisions;

Declares the claim admissible and substantiated, to the following extent:

Orders the defendants, the company under the law of the State of Delaware (United States of America) FACEBOOK, INC., FACEBOOK BELGIUM SPRL, and the company under Irish law FACEBOOK IRELAND LIMITED, in respect of every Internet user on Belgian territory who has not registered as a member of the online social network of Facebook, to cease:

- placing a datr cookie when they land on a web page of the facebook.com domain without providing them with prior sufficient and adequate information about the fact that Facebook places the datr cookie with them and about the way Facebook uses that datr cookie through social plug-ins;
- collecting the datr cookie through social plug-ins placed on third-party websites.

Sentences the defendants, the company under the law of the State of Delaware (United States of America) FACEBOOK, INC., FACEBOOK BELGIUM SPRL, and the company under Irish law FACEBOOK IRELAND LIMITED, to pay to the plaintiff, Mr WILLEM DEBEUCKELAERE, pursuant to Article 32, § 3 of the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, acting in his capacity of PRESIDENT OF THE BELGIAN COMMISSION FOR THE PROTECTION OF PRIVACY, a fine of EUR 250,000 per started period of 24 hours in which this order for cessation is not complied with;

Rejects the other claims;

Furthermore sentences the defendants, , the company under the law of the State of Delaware (United States of America) FACEBOOK, INC., FACEBOOK BELGIUM SPRL, and the company under Irish law FACEBOOK IRELAND LIMITED, to the costs of the proceedings, estimated at € 459.99 for issuing the summons and € 1,320.00 by way of compensation towards the administration of justice

for Mr WILLEM DEBEUCKELAERE, acting in his capacity of PRESIDENT OF THE BELGIAN COMMISSION FOR THE PROTECTION OF PRIVACY;

Declares this decision immediately enforceable by operation of law and without any security.

Thus pronounced and sentenced at the public hearing of 9 November 2015.

[signed]	*[signed]*
C. KINT	W. THIERY