# Submission by „Facebook Ireland Ltd“
# to the Office of the Irish Data Protection Commissioner

**Response to Complaint(s) Number: 17**

The following submission by “Facebook Ireland Ltd” is a response to complaints filed by “europe-v-facebook.org” before the Irish Data Protection Commissioner as amended by our “request for a formal decision”. It was received by “europe-v-facebook.org” on September 30th 2013.

The submission starting on page 2 of this PDC does only reflect the view of “Facebook Ireland Ltd” and was not changed or amended. The submissions were likely drafted by Facebook Ireland’s law firm “Mason, Hayes & Curran”. We did not receive any addition documents from “Facebook Ireland Ltd”. All other documents of this procedure can be downloaded on “europe-v-facebook.org”.

**After we took a first look at the submissions by “Facebook Ireland Ltd” we want to mention the following points, to ensure that any reader will get the full picture of the procedure:**

1. In the submissions Facebook Ireland Ltd does in many cases **not responded to our complaints**, but produced arguments and submissions that are irrelevant to the complaints filed. It seems that Facebook Ireland Ltd is trying to “bypass” the arguments we entertained.

2. In the submissions Facebook Ireland Ltd does in many cases **summarize our complaints** in a way that does not reflect the content of our complaints. We do not know why Facebook Ireland Ltd has chosen this approach other then again “bypassing” the core of the complaints.

3. In the submission Facebook Ireland Ltd does not respond to the **legal arguments** that were submitted by us, but only focus on facts. The law is not cited in any of the submissions.

4. In the past 2 years Facebook Ireland Ltd has changed many functions. In the submissions Facebook Ireland Ltd does in many cases **mix the factual situation** throughout this time period. Our complains are usually separating facts and consequences before and after such changes.

5. In the submission Facebook Ireland Ltd does in many cases refer to the “**audit reports**”. The basis for these reports is not public or independently verifiable. In many cases the DPC has only relied on unverified arguments by Facebook Ireland Ltd when making its assessment. Facebook Ireland Ltd is now relying on these findings, as if they were independently verifiable facts.

➔ **Therefore we recommend to consult our original complains, as amended by the “request for a formal decision” [DOWNLOAD] when analyzing the submissions from “Facebook Ireland Ltd”.**

## COMPLAINT 17 – LIKE BUTTON and SOCIAL PLUGINS

## 1. INTRODUCTION

### 1.1. What are social plugins?

Social plugins – such as the "like" button – which are found on many popular websites, allow web developers to embed Facebook content into their websites. These plugins allow Facebook users visiting a website to interact with that site and to share content on that site with their Facebook friends.

### 1.2. Data Use Policy

FB-I's Data Use Policy contains a clear explanation as to how social plugins such as the "like" button work on Facebook. FB-I clearly sets out the purposes to which it may put the information it collects in the 'How We Use The Information We Receive' section:

> *We use the information we receive about you in connection with the services and features we provide to you and others like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.*

In the 'Other Information We Receive About You' section of the Data Use Policy, the following information is provided to users:

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

The 'About Social Plugins' section of the Data Use Policy provides the following comprehensive description of social plugins:

> *Social plugins are buttons, boxes and stories (such as the Like button) that other websites can use to present Facebook content to you and create more social and personal experiences for you. While you view these buttons, boxes and stories on other sites, the content comes directly from Facebook.*
>
> *Sometimes plugins act just like applications. You can spot one of these plugins because it will ask for your permission to access your information or to publish information back to Facebook. For example, if you use a registration plugin on a website, the plugin will ask your permission to share your basic info with the website to make it easier to register with the website. Similarly, if you add an 'Add to Timeline' plugin, the plugin will ask your permission to publish stories about your activities on that website to Facebook.*
>
> *If you make something public using a plugin, such as posting a public comment on a newspaper's website, then that website can access your comment (along with your user ID) just like everyone else.*
>
> *If you post something using a social plugin and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a Facebook comment plugin on a site, your story is Public, and everyone, including the website, can see your story.*
>
> *Websites that use social plugins can sometimes tell that you have engaged with a social plugin. For example, they may know you have clicked on a Like button in a social plugin.*
>
> *We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with another individual's data in a way that it is no longer associated with you. Learn more at: https://www.facebook.com/help/social-plugins*

FB-I's Data Use Policy provides further information to users in relation to the manner in which cookies are placed by FB-I and the uses to which those cookies are ultimately put. Part V of the Data Use Policy is entitled '*Cookies, Pixels and Other Technologies*' and clearly states that these technologies are used by Facebook for the following purposes:

> *We use these technologies to do things like:*
>
> > **make Facebook easier or faster to use;*
> >
> > **enable features and store information about you (including on your device or in your browser cache;*
> >
> > **deliver, understand, and improve advertising;*
> >
> > **monitor and understand the use of our products and services; and*
> >
> > **to protect you, others, and Facebook.*
>
> *For example, we may use them to know you're logged in to Facebook, to help you use social plugins and share buttons or to know when you're interacting with our advertising or Platform partners.*

### 1.3. Help Center

In addition to the information which is provided by the Data Use Policy, Facebook provides further guidance in relation to the operation of social plugins in its Help Center which contains the following explanation of plugins:

> *How do social plugins work?*
>
> *While social plugins appear on other websites, the content populating them comes directly from Facebook – so they're just an extension of your Facebook experience. Plugins were designed so that the website you are visiting receives none of this information.*
>
> *You only see a personalised experience with your friends if you are logged into your Facebook account. If you are not already logged in, you will be prompted before you can use a plugin on another site.*
>
> *At a technical level, social plugins work when external websites put an iframe from Facebook.com on their sites, as if they were agreeing to give Facebook some real estate on their websites. When you visit one of these sites, the Facebook iframe can recognise if you are logged into Facebook. If you are logged in, it'll show personalised content within the plugin as if you were on Facebook.com directly. Even though the iframe is not on Facebook, it is designed with all the privacy protection as if it were.*

### 1.4. Cookies Policy

In addition, FB-I's Cookie Policy, which was originally published in June 2012, provides information on how cookies are used in association with social plugins:

> *Why do we use these technologies?*
>
> …
>
> *Authentication These tools tell us when you're logged in, so we can show you the appropriate experience and features.*
>
> *For example, cookies, local storage and similar technologies tell us when you are logged in to Facebook so we can show you relevant and social information when you visit other websites that use our social plugins. We also use this information to understand how people use our Platform and other apps and services.*

…

*Analytics and research These are used to understand, improve, and research products and services, including when you access Facebook or other websites and apps from a computer or mobile device.*

*For example, we may use cookies to understand how you are using social plugins to improve them. We and our partners may use these technologies and the information we receive to improve and understand how you use websites, apps, products, services and ads. We may share information about this analysis with our partners.*

## 2. FACTUAL ASSERTIONS MADE BY THE COMPLAINANT

The Complainant objects to the manner in which social plugins operate. In the Original Complaint, the Complainant alleges the following:

a) *'Social plug-ins' are used to "track the users around the web".*

b) *Plug-ins are not only found on 'normal' pages but may also be found on pages which contain sensitive information relating to political and religious views, health and sex. As the user is not informed in advance of accessing a web-page whether or not that page contains a social plug-in, sensitive information of web-users could be inadvertently provided to Facebook without that web-user's consent.*

c) *Facebook gathers the following information each time a user visits a site which has a social plug-in, even where the data subject does not interact with the plug-in in any way: date, time, URL and 'other technical information' including the IP address, browser and operating system information.*

d) *Facebook Ireland also places cookies in a user's browser's cache each time a user interacts with Facebook and these permit Facebook to track individual users for a period of two years, unless that user chooses to delete his/her cookies.*

e) *The data collected by Facebook in this manner is part of an integrated network of data which is not stored in the EEA but in the US and that therefore, FB-I does not guarantee the security of such data as it is required to do pursuant to the Data Retention Directive. The Complainant further asserts that FB-I is in breach of the Data Retention Directive on the basis that there is no guarantee that US or European law enforcement agencies do not access the sensitive information of European citizens hosted by FB-I.*

In the Request for Formal Decision[1], the Complainant further alleges that:

f) *FB-I has now relied on at least four reasons for the manner in which cookies and social plugins operate on the Facebook platform. The Complainant contends that this calls into question the credibility of FB-I relying on any of its stated reasons for retaining these data.*

g) *The Technical Analysis Report does not definitively prove that there is no correlation between the targeting of advertising at users, and the data generated by the use of cookies and social plugins.*

h) *There are indications of the purpose for which these data are used, but no solid evidence to identify that purpose.*

The DPC's analysis of FB-I's data use in the audit, re-audit and the two technical reports shows the Complainant's allegations to be without merit.

The purpose of the like button and other social plugins is to allow Facebook users to have personalised social experiences while browsing third-party sites and to be able to connect those experiences with their activity and friends on Facebook.

[1] Page 61 of Request for Formal Decision

## 3. AUDIT PROCESS

### 3.1. Introduction

The DPC set out its understanding of the Complainant's allegations in the following terms:

> *This is an issue which was also the subject of complaint from Europe-v-Facebook, Complaint 17 – Like Button. The complainant stated that when a user visits a website which contains a 'social plug in' – the Like button – the following information is being recorded: date, time, URL, IP address, browser and operating system information. The complainant considers that the information is being collected unfairly and is excessive and allows Facebook to track user movements across the web.*[2]

The DPC conducted an extensive analysis of FB-I's use of social plugins throughout the audit. This assessment had two distinct components.

First, the DPC considered whether FB-I was using social plugins for profiling purposes.

Second, the DPC considered FB-I's approach to cookie management and the retention of data derived from social plugins.

### 3.2. Use of social plugin data

Having engaged in extensive technical investigations, the DPC was satisfied that FB-I did not use social plugins for profiling purposes.

#### 3.2.1. 2011 Audit Report

The DPC opened its consideration of this issue with the following general observation:

> *Facebook, like almost every website, also drops cookies (text containing a piece of information) when a person visits Facebook.com. This is a standard practice on the internet.*[3]

The DPC also gave the following explanation of the workings of social plugins in the 2011 Audit Report:

> *Social plugin content is loaded in an inline frame or iframe. An iframe allows a separate HTML document to be loaded while a page is being loaded. In this case, the social plugin content is loaded separately from the content of the surrounding website. This is a standard way that content from different publishers is loaded to a website. When a user visits one of these sites, the Facebook iframe can recognise if the user is logged into Facebook. If the user is logged in, the website will show personalised content within the plugin as if the user were on facebook.com directly.*[4]

Turning first to the allegations that FB-I was profiling *non-users*, the DPC noted that for non-Facebook users who had never visited Facebook, no cookies were either set or read by FB-I when visiting a website with a social plugin. The browser's IP address is collected but this was done simply to permit the inline frame to deliver the social plugin.[5]

This is in line with the findings of the 2011 Technical Audit Report, prepared by the DPC's expert, which noted that:

---

[2] Page 83 of the 2011 Audit Report
[3] Page 81 of the 2011 Audit Report
[4] Page 81 of the 2011 Audit Report
[5] Page 81 of the 2011 Audit Report

> *Therefore, in this case, where the non-Facebook user has never visited www.facebook.com, no cookies are sent either to or by Facebook when a user visits websites containing social plug-ins.*[6]

Earlier on in the 2011 Audit Report, the DPC also confirmed that FB-I was not seeking to profile non-users:

> *As outlined in the Technical Analysis Report, this Office is satisfied that while certain data which could be used to build what we have seen termed as a "shadow profile" of a non-user was received by Facebook, we did not find that any actual use of this nature was made of such data and as outlined elsewhere in this report, FB-I is now taking active steps to delete any such information very quickly after it is received, subject to legal hold requirements The receipt of such data is in most cases attributable to the way the internet works with different content on websites delivered by different content providers. A Facebook social plugin embedded in a website is delivered by Facebook directly to the user's computer when a user visits that website with the means of delivery the IP address of the user's machine.*[7]

In other words, the DPC considered, and comprehensively rejected, the allegation that FB-I was using social plugins to profile *non-users*.

The DPC came to the same conclusion with respect to data derived from social plugins on sites visited by *users*.

During the audit, the DPC was given wide-ranging access to the FB-I log entries and the code which logs social plugin impressions. On foot of this code review, the DPC concluded as follows:

> *The structure of Facebook log entries was reviewed as well as the code that performs logging. Access was sought and provided to the log entries, the code used to query the entries and the queries made to the logs and we were satisfied that no access was made to any information that could be considered to be personal data in the logged information for advertising or profiling purposes.* [8]

The DPC then proceeded to examine the link, if any, between the information received by Facebook when data subjects visit webpages with social plugins and the advertisements which are presented to the user. The DPC concluded that *"[n]o correlation with browsing activity was found".*[9]

This finding is corroborated by the 2011 Technical Audit Report which details at pages 184 to 185 the tests which were undertaken to identify any potential link between advertising and the operation of social plugins. The 2011 Technical Audit Report concluded that:

> *The act of browsing to websites containing social plugins does not appear to have any influence on the advertising targeted at the user.*[10]

Facebook's position in respect of its use of cookies and social plugins for targeting advertising was clearly set out by the DPC:

> *FB-I stated that it has not designed its systems to track user and non user browsing activity and that users have provided consent for the processing of data. FB-I contended that it provides 'exhaustive' information in relation to the use of 'social plug ins'*
>
> > *When you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time, and other browser-related information.*

---

[6] Page 174 of the 2011 Technical Audit Report
[7] Page 52 of the 2011 Audit Report
[8] Page 83 of the 2011 Audit Report
[9] Page 83 of the 2011 Audit Report
[10] Page 185 of the 2011 Technical Audit Report

> *If you don't have a Facebook account and visit a website with the Like button or another social plugin, your browser sends us a more limited set of information. For example, because you're not a Facebook user, we don't receive a user ID. We do receive the webpage you're visiting, the date and time, and other browser-related information. We record this information for a limited amount of time to help us improve our products.*[11]

The DPC was satisfied that the data collected by FB-I, either through the use of cookies or through the use of social plugins, was not improperly associated with Facebook users. The DPC stated as follows:

> *Our task therefore was to satisfy ourselves that no such use was made of the collected data. We are satisfied in this point.*[12]

The DPC concluded its assessment of this issue by noting that:

> *We are satisfied that no use is made of data collected via the loading of Facebook social plug-ins on website for profiling purposes of either users or non-users.*[13]

### 3.2.2. 2012 Audit Report

The DPC's external expert again tested social plugins in advance of the 2012 Audit Report and the results of those tests are set out at paragraphs 1.5.8 and 1.5.9 of the 2012 Technical Audit Report, which corroborate the findings of the 2011 Technical Audit Report. The findings of the 2012 Technical Audit Report were stated to be *'consistent'* with the findings of the 2011 Technical Audit Report.

In particular, the 2012 Technical Audit Report concluded as follows:

> *The act of browsing to websites containing social plugins does not appear to have any influence on the advertising targeted at a user.*[14]

After reciting the findings of the 2011 Audit Report that social plugin data is not used for profiling purposes, the DPC noted:

> *The process for re-testing this issue is outlined at section 1.5.8 of the 2012 Technical Audit Report. Over 2000 queries served in one particular month to the retained social plug-in data were examined and we were satisfied that no user or non-user was queried.*[15]

This process is described in the 2012 Technical Audit Report:

> *During this audit, all social plugins queries performed during a second random month long period were examined. All individual object IDs (210) in total were examined and it was confirmed that none represented Facebook users.*
>
> *It is therefore concluded that the examined information continues to indicate that no individual user or non-user browsing activity is being extracted from social plugin logs for analysis.*[16]

For the sake of completeness, it should be noted that the 2012 Audit Report found that a new cookie used by Facebook, the "fr" cookie, could be used by FB-I to monitor browsing of users and that steps needed to be taken in relation to legitimising this cookie. The DPC expressed its expectation that FB-I

---

[11] Page 83 of the 2011 Audit Report
[12] Pages 84 to 85 of the 2011 Audit Report
[13] Page 86 of the 2011 Audit Report
[14] Page 38 of the 2012 Technical Audit Report
[15] Page 28 of the 2012 Audit Report
[16] Page 38 of the 2012 Technical Audit Report

would supply more information to the DPC in relation to the functioning of the "fr" cookie within a period of four weeks from the date of the 2012 Audit Report.

This issue was subsequently resolved to the satisfaction of the DPC, as noted at page 19 of the DPC's 2012 Annual Report.

### 3.2.3. Use of social plugin data - conclusion

The DPC carried out two sets of extensive technical tests and found no correlation between browsing activity on websites which contain social plugins and the targeting of advertising at Facebook users. This testing included the analysis of thousands of queries which had been run against Facebook's social plugin logs over a certain period of time together with randomised testing of advertising trends when users have accessed websites with social plugins. Those findings comprehensively highlight the inaccuracy of many of the Complainant's complaints on this issue.

## 3.3. Retention of data

### 3.3.1. 2011 Audit Report

In the course of the 2011 audit, the DPC focussed considerable attention on the management by FB-I of its cookie and social plugin data and on the length of time this information is retained by FB-I. The DPC noted the engineering and technical efforts made by FB-I in this regard and stated as follows:

> *The Facebook security team have demonstrated a recently improved feature for practice management of browser cookie state, known as "Cookie Monster". The code of this feature was reviewed and confirmed to operate as described in the Technical Analysis Report.*[17]

This newly introduced feature was examined in the 2011 Technical Audit Report, which detailed the difficulties which previously arose from the manual management of cookies:

> *Historically, the deletion of cookies on logout required manual insertion of code into the logout process to unset each cookie. The technique was error prone, since developers could add a new cookie but forget to add the corresponding code to unset the cookie on logout.*[18]

By contrast, the newly automated *"Cookie Monster"* process was described as follows:

> *The cookie management framework is executed on every Facebook request, including requests from social plugins. Unexpected cookies, or cookies from the incorrect context (such as cookies that are only meaningful in the context of a logged-in user being received in a request from a non-logged in user), are automatically unset.*[19]

The DPC therefore concluded that the new framework would reduce the amount of data held by FB-I. It stated:

> *It can be assumed that this framework will serve to assist Facebook in combating the collection of excessive information via cookies which were initially intended for another more limited purpose.*[20]

The 2011 Audit Report further noted that FB-I had agreed to reduce the period for time for which it held data derived from social plugins:

---

[17] Page 84 of the 2011 Audit Report
[18] Page 181 of the 2011 Technical Audit Report
[19] Page 182 of the 2011 Technical Audit Report
[20] Page 84 of the 2011 Audit Report

*FB-I has confirmed to this office that, as part of its commitments described below, it will be amending its data retention policy for social plugin impression logs to provide enhanced protection to the information of users and non-users. Specifically, under its revised policy, for people who are not Facebook users or who are Facebook users in a logged out state, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com. In addition, for all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin. These combined measures ensure that FB-I retains information stored in social plugin logs for a minimal period of time.*[21]

The DPC therefore made a best practice recommendation that FB-I revise its data retention policy in respect of cookies and social plugins so that the information which FB-I receives by those means is kept for a very short period and for a limited purpose.

### 3.3.2. 2012 Audit Report

In the 2012 Audit Report, the DPC restated its recommendations to FB-I with respect to a reduction in the retention periods for data derived from social plugins:

> ***Recommendation: FB-I will comply with requirements in relation to retention where the company no longer has a need for the data in relation to the purposes for which it was provided or received. Specifically it will:***
>
> ***1. For people who are not Facebook users or who are Facebook users in a logged out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com.***
>
> ***2. For all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin.***[22]

The 2012 Audit Report went on to note that FB-I had complied with these recommendations.[23]

### 3.3.3. Retention of data – conclusion

In light of the DPC's recommendations, FB-I has overhauled aspects of its approach to retaining data derived from social plugins. Such data is now managed fully in line with the DPC's recommendations.

## 4. APPLICATION TO CURRENT COMPLAINT

In light of the above, FB-I responds to the specific factual assertions made by the Complainant as follows:

*a) 'Social plug-ins' are used to "track the users around the web".*

This has been demonstrated by the DPC to be untrue. The technical reports have clearly shown how FB-I processes the information that is transmitted to FB-I when either a user or non-user browses a site with

[21] Page 85 of the 2011 Audit Report
[22] Page 24 of the 2012 Audit Report
[23] Page 25 of the 2012 Audit Report

a social plugin. The technical analysis further shows that there is no correlation between web-users navigating to sites with social plugins and the advertisements which are presented to that user.

*b) Plug-ins are not only found on 'normal' pages but may also be found on pages which contain sensitive information relating to matters such as politics, religion, health and sex. As the user is not informed in advance of accessing a web-page whether or not that page contains a social plug-in, sensitive information of web-users could be inadvertently provided to Facebook without that web-user's consent.*

The technical reports have clearly shown how FB-I processes the information that is transmitted to FB-I when either a user or non-user browses a site with a social plugin. These reports show that FB-I does not extract or specifically process sensitive data as alleged.

*c) Facebook gathers the following information each time a user visits a site which has a social plug-in, even where the data subject does not interact with the plug-in in any way: date, time, URL and 'other technical information' including the IP address, browser and operating system information.*

FB-I accepts that information is transmitted when users and non-users visit a website with a social plugin; this is a by-product of the operation of the internet. This matter was dealt with comprehensively at pages 82 and 83 of the 2011 Audit Report. FB-I deletes or depersonalises this information within 10 days in respect of non-users and within 90 days in respect of logged-in users. This was confirmed by a code review referred to at page 25 of the 2012 Audit Report and page 52 of the 2012 Technical Audit Report.

*d) Facebook Ireland also places cookies in a user's browser's cache each time a user interacts with Facebook and these permit Facebook to track individual users for a period of two years, unless that user chooses to delete his/her cookies. The Complainant claims not to understand the benefit to Facebook of collecting these data nor does he believe that the data can in any way improve the performance of the Facebook platform.*

As the 2011 Audit Report noted[24], almost every website on the internet drops cookies on web-users' browsers when a site is visited. The different cookies used by FB-I have been examined in great detail by the DPC and have been detailed in the technical analysis reports; none of the cookies analysed were found to track users around the web. The Cookie Monster system was also recognised by the DPC as having improved the management by FB-I of cookies.

*e) The data collected by Facebook in this manner is part of an integrated network of data which is not stored in the EEA but in the US and that therefore, FB-I does not guarantee the security of such data as it is required to do pursuant to the Data Retention Directive. The Complainant further asserts that FB-I is in breach of the Data Retention Directive on the basis that there is no guarantee that US or European law enforcement agencies do not access the sensitive information of European citizens hosted by FB-I.*

FB-I has addressed the security of its data in its Response to Complaint 12 – 'Data Security'. FB-I's policy in respect of disclosure of information to third parties can be found at pages 98 to 100 of the 2011 Audit Report and is further dealt with elsewhere in these Reponses, in particular in the Response to Complaint 7 – 'Messages'.

*f) FB-I has now relied on at least four reasons for the manner in which cookies and social plugins operate on the Facebook platform. The Complainant contends that this calls into question the credibility of FB-I relying on any of its stated reasons for retaining these data.*

The reasons for which FB-I collects data in relation to cookies and social plugins are plainly disclosed to users both in the Cookies Policy and the Data Use Policy. This was also examined and confirmed by the DPC during the audit.

[24] Page 81 of the 2011 Audit Report

*g) The Technical Analysis Report does not definitively prove that there is no correlation between the targeting of advertising at users, and the data generated by the use of cookies and social plugins.*

The DPC concluded after extensive technical examination, that no correlation could be found between social plugins and the targeting of advertising.[25]

*h) There are indications of the purpose for which these data are used, but no solid evidence to identify that purpose.*

The purposes for which FB-I uses social plugins have been set out above and were subject to technical examination by the DPC during the audit process.

[25] Page 83 of the 2011 Audit Report