

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

### Response to Complaint(s) Number: 2

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 30<sup>th</sup> 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 2 – SHADOW PROFILES

### 1. BACKGROUND

FB-I does not create “shadow profiles” of its users, or “profiles”, of any sort, of non-users. The various allegations made by the Complainant have either been disproved by the DPC during the audit or are false and misleading.

### 2. FACTUAL ALLEGATIONS

In the Original Complaint, the Complainant alleges the following:

- (a) *FB-I creates “shadow profiles” of its users and non-users.*
- (b) *FB-I uses social plugins to build “shadow profiles” of both users and non-users.*
- (c) *FB-I scans message content to build “shadow profiles” of its users.*
- (d) *FB-I uses synchronised and imported contacts to build “shadow profiles” of its users.*

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

- (e) *FB-I uses inferred profile completion questions to build “shadow profiles”.*
- (f) *It is possible for a user who creates a new profile to infer the friends list of another user, even if that latter user has hidden their friends list.*
- (g) *FB-I is using content provided by other users about their friends to build “shadow profiles”.*
- (h) *FB-I is using Facebook Exchange to build “shadow profiles”.*
- (i) *FB-I is using Partner Categories to build “shadow profiles”.*
- (j) *FB-I is using publicly available information, particularly that taken from Wikipedia, to build “shadow profiles”.*

### 3. AUDIT PROCESS

#### 3.1. Introduction

In the 2011 Audit Report, the DPC set out its understanding of the Complainant’s allegations of “shadow profiles”:

***Complaint 2 – Shadow Profiles** the complainant stated that Facebook is gathering information in relation to users and non-users of Facebook through a number of functions including the synchronisation of mobile phones, importation of personal data from email contact lists, instant messaging services and through invitations sent to friends. This information primarily consists of email addresses, but may also include names, telephone numbers and addresses. The complainant contended that the information is being used to add to Facebook’s information in relation to users and to create shadow profiles of non-users of Facebook without the knowledge of the data subject. The complainant added that some of this information may be of embarrassment to the data subject.*

*In response to his access request to Facebook, the complainant stated that he did not receive any information in relation to other people who may have uploaded his personal data to Facebook through synchronising their mobile device or uploading their email contact list.*

*The complainant considered that Facebook is in breach of a number of areas of data protection legislation, including the fair processing principle and that the collection of the data is excessive. In addition, he stated that Facebook's Privacy Policy does not contain any notice to inform users that shadow profiles are held, for what purpose they are being used and that non-users have not given their consent for the retention and processing of this data.<sup>1</sup>*

### 3.2. Summary of DPC findings

During the audit, the DPC considered, and unequivocally dismissed, a number of the “shadow profile” allegations now raised by the Complainant.

It is important to recall that the DPC came to this view with the benefit of extensive technical testing (as set out in the 2011 and 2012 Technical Audit Reports) and full access to the data held by FB-I.

As the 2011 Audit Report noted:

*A significant proportion of the audit was therefore focused on establishing the extent of personal data held by FB-I and whether any of the limited exemptions contained within the Data Protection Acts could be validly claimed by FB-I. We are satisfied that we had full access to all data relating to users and non-users held by FB-I.<sup>2</sup>*

The DPC's consideration of these various allegations are set out in length in our various Responses, particularly FB-I's Responses to Complaint 4 – ‘Synchronizing’, Complaint 7 – ‘Messages’, Complaint 10 – ‘Subject Access Requests’, Complaint 15 – ‘Excessive Processing’ and Complaint 17 – ‘Like Button’. These Responses should be read as forming part of FB-I's Response to this Complaint.

For ease of reference, the DPC's clear findings on these points are set out below.

First, in light of the modifications which FB-I had made between the 2011 and 2012 audits, the DPC accepted that FB-I was providing users with proper access to their personal data:

*With the exception of the photograph metadata we are satisfied that all users are now receiving access to their personal data held by FB-I in a manner that complies fully with the obligations placed under FB-I by Sections 3 and 4 of the Data Protection Acts.<sup>3</sup>*

Second, FB-I's scanning of messages is limited to child protection. FB-I does not derive information about its users by scanning their messages.

*FB-I has clarified that it does not conduct ad-targeting based on the content of messages and chat on the site.<sup>4</sup>*

Third, social plugins are not being used to profile individuals:

*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.<sup>5</sup>*

Fourth, synchronised data is stored on behalf of the uploading user and is used for friend-finding purposes only:

*We are satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder purposes.<sup>6</sup>*

---

<sup>1</sup> Page 119 of the 2011 Audit Report

<sup>2</sup> Page 64 of the 2011 Audit Report

<sup>3</sup> Page 22 of the 2012 Audit Report; note: photo metadata is now provided.

<sup>4</sup> Page 18 of the 2012 Audit Report

<sup>5</sup> Page 86 of the 2011 Audit Report

<sup>6</sup> Page 125 of the 2011 Audit Report

## 4. ADDITIONAL ALLEGATIONS

In the Request for Formal Decision, the Complainant makes a number of additional points which he alleges support his original allegations (rejected by the DPC) that FB-I holds “shadow profiles”.

### 4.1. Profile completion questions

As the Complainant notes, FB-I sometimes prompts its users to complete their timeline on the site (such as by suggesting their hometown). This function is entirely transparent and clearly visible to the average user of Facebook. Suggestions are cached for limited periods of time and, as the DPC confirmed, such suggestions are not influenced by the content of messages. In these circumstances, users can either ignore the question or answer the question to augment their timeline.

### 4.2. Friend suggestions

FB-I makes friend suggestions to its users. Again, this is a transparent part of the platform. Like timeline completion questions, friend suggestions are cached for limited periods of time

While FB-I fails to see the relevance of this point to the allegation of “shadow profiles”, the Complainant alleges that if a new account is set up and adds a single friend the entire friend list of that single friend could be seen by the new user in “friend suggestions” (even if the friend has chosen to hide his/her friend list). First, as a clarification, a user’s “friend list” is not shown to new users. Second, friend suggestions may contain the friends of a friend a new user has added because it is likely that he/she may know or wish to friend such people. But, regardless, those friend suggestions are not attributed to a particular friendship and, in any event, no information is shared with the user (beyond what they could see on their own).

Importantly, regardless of the product functionality described above, the Data Use Policy expressly informs users about the effects of audience selection for friends lists, including how users can control the visibility of their friend list (on their timeline):

*When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public," anyone will be able to see your connection on your friend's timeline.*

### 4.3. Data provided by users’ friends

The Complainant alleges that FB-I obtains information from users’ friends, which in turn is used to create a “shadow profile” of a user. The Complainant alleges that Facebook users are “spying” on each other.

FB-I utterly rejects any allegation that users “spy” on each other on its behalf. Facebook is a social network, based on sharing content and information. Given the social nature of the platform, Facebook users can involve their friends in their posts. If a Facebook user did something with one of their Facebook friends (such as attend college together), they may tag that friend in the relevant posting. This functions in the same as any other tag and can be removed and deleted by the tagged user in the normal way. When people share a post on Facebook, they choose whom to share that post with, and they can delete the post or change the audience anytime.

### 4.4. Facebook Exchange (“FBX”)

The Complainant alleges that FB-I uses FBX, a type of real time bidding for advertising on Facebook, to generate “shadow profiles”.

FBX, and the associated “fr” cookie which supports it, was subject to technical examination by the DPC during the 2012 Audit. While the DPC suggested that FB-I may need to consider refining its disclosures in this area, it did not regard this technology as in any way creating “shadow profiles” or generating personal data which needed to be disclosed in response to a subject access request. Since the audit, FB-I has increased the information available to users, including by clicking on the word “sponsored” or clicking on the “about this ad” link from the ad itself. These resources explain more about FB-I’s advertising products and how to use the controls available.

#### 4.4.1. What is FBX?

FBX gives marketers an opportunity to bid on showing ads in real time. Approved third-party service providers work with FB-I and marketers to enable this process. FB-I agrees with a provider on an ID number (separate from a Facebook ID) for each visitor’s browser. If someone then visits Facebook and his or her browser has that ID, FB-I notifies the service provider, who tells FB-I when a marketer wants to show a particular ad.

As is more fully explained in Section 4.4.2 of this Response (which sets out the relevant extracts from the 2012 Technical Audit Report) this process is driven via a partner’s pixel tag placed on a third party website and a cookie dropped by Facebook (on logged in Facebook users).

FBX allows marketers to bid to show ads to the user that are relevant to the user’s existing relationship with the product being advertised, *without* the marketer being required to provide FB-I with personal information about the user.

When FB-I shows an FBX ad on Facebook, it includes an ‘x’ link that lets users provide feedback about ads. FB-I also provides a link that lets users learn more about and choose to opt-out of future ads from the service provider responsible for that ad. In addition, FB-I only works with providers that agree to technical and policy requirements that protect the privacy of personal information.

This practice is disclosed in FB-I’s Cookie Policy:

*We also may work with a partner to show you an ad on or off Facebook, such as after you’ve visited the partner’s site or app and this may involve the use of cookies, local storage on your device or other similar technologies.*

In short, FBX has been built from the ground up to prevent FB-I from obtaining additional information about its users. In addition, this technology was considered by the DPC during the 2012 audit.

#### 4.4.2. 2012 Technical Audit Report

The 2012 Technical Audit Report described the functionality of FBX in the following terms:

*As part of the testing carried out for this audit, a new cookie named fr was identified.*

*It was noted that the cookie is only set when a Facebook user logs in to the site and it has an expiry period of 30 days. The cookie, including the encrypted user id, is retained after the user logs out. Upon examination, the fr cookie clearly consists of two components.*

*An example fr cookie value is*

*“Onx07ppspaoOQ!Qv1.AWVAlyAiGNl9vuExmcrX2lmfAfk”.*

*Facebook were asked to provide an explanation of the purpose of this new cookie.*

*The content of the two parts of the cookie have been reported to be as follows;*

- *The first part of the cookie is a browser ID, used to identify the web browser.*

- *The second part of the cookie is an encrypted version of the logged in user's Facebook ID. The user's ID is re-encrypted every hour to a different value.*<sup>7</sup>

*The code used to generate the fr cookie value has been reviewed and it has been confirmed that the browser ID is a random value and the encrypted user ID value contains only the Facebook user ID. It was also confirmed by code review that the fr cookie value generation code is called whenever the other login session cookie values (c\_user, xs, etc.) are refreshed, which takes place roughly hourly but this can vary for operational reasons.*

*This cookie is being used by Facebook to deliver a series of new advertisement products such as real time bidding, which works as follows:*

- *An advertising partner of Facebook, for example, doubleclick has an ad on, for example, the New York Times website*<sup>8</sup>.
- *A Facebook user visits the New York Times.*
- *The website contains a pixel image which causes a request to be sent to Facebook. Usually, the request to Facebook will have a referrer value of the partner (in this case doubleclick), along with an opaque partner value provided by doubleclick. In some cases, partners do not control the browser referrer value. In such cases, FB-I states that they exclude this referrer value from their impression logs and do not use it as part of this or other advertising systems.*
- *Facebook store a relationship between the partner value and the fr cookie browser component value.*
- *Then, when the user visits Facebook, the partner is sent the partner value and can respond with a bid amount to bid to have an ad displayed to the user.*
- *If the partner wins the bid, Facebook will serve a standard ad from a standard ad campaign to the user.*

*To summarise what each of the actors know about the user's activity:*

- *The partner (doubleclick in this case) knows that the user has visited the New York Times website.*
- *Facebook do not know that the user has visited the New York Times website*<sup>9</sup>. *The meaning of the partner value provided to Facebook is opaque to Facebook. FB-I report that the partner values are typically short identifiers. While this value may, hypothetically, somehow encode the fact that the user has visited the New York Times website it is not clear how or why the partner would choose to do this. The partner will store whatever data they know about the user in their own database.*<sup>10</sup>
- *Facebook know information about the user provided separately by the user to Facebook (e.g. the user's profile information).*
- *The partner has no access to any information provided by the Facebook user to Facebook.*
- *Due to the bid requests, the partner may know which browsers are active Facebook users, but they are contractually prohibited from storing or using this fact.*

*Although this cookie will be sent in requests for social plugins that occur after a browser has had a logged in user, FB-I states that this cookie is not currently used other than as described above.*<sup>11</sup>

It is important to highlight the fact that the 2012 Technical Audit Report confirmed that FBX does not provide FB-I with additional information about its users:

*Facebook do not know that the user has visited the New York Times website. The meaning of the partner value provided to Facebook is opaque to Facebook.*<sup>12</sup>

#### 4.4.3. 2012 Audit Report

<sup>7</sup> Page 33 of the 2012 Technical Audit Report

<sup>8</sup> *With the exception of Facebook, the actors described in the following example are intended purely to illustrate the functionality of the cookie. It is not known, nor is it relevant, whether doubleclick is an advertising partner of Facebook or whether doubleclick have an ad on the New York Times website.*

<sup>9</sup> *As mentioned above, sometimes FB-I may receive this value in a HTTP referrer header but they have stated that they do not log the referrer value from such requests.*

<sup>10</sup> Page 34 of the 2012 Technical Audit Report

<sup>11</sup> Pages 33 to 35 of the 2012 Technical Audit Report

<sup>12</sup> Page 34 of the 2012 Technical Audit Report

The DPC considered FBX in its 2012 Audit Report. The DPC expressed no concerns that FBX would lead to the creation of “shadow profiles” but simply noted that, due to the use of the fr cookie, it is important that proper consent be obtained:

### **Cookies**

*A detailed re-examination of the use of cookies on Facebook was conducted and is contained in Section 1.5.4 of the Technical Analysis Report. The position as outlined in the December audit has remained broadly the same with the exception of a cookie termed "fr". The purpose of this cookie is outlined at Section 1.5.5.14 of the Technical Analysis Report. As it is a cookie that FB-I is using in order to monitor browsing by users and not for a security purpose, the initial view of this Office is that it falls to be considered as a cookie for which a consent in line with the provisions of Statutory Instrument 336 of 2011 is required. The exact form that such a consent should take is a matter that remains under discussion among enforcement authorities and industry and we expect FB-I to implement whatever that solution is.*

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

### **Action**

*FB-I to supply more detailed information to this Office within four week's of today's date on the use of the fr cookie and the consent collected for the cookie that is dropped to support such advertising.<sup>13</sup>*

This issue was subsequently progressed to the satisfaction of the DPC, as is noted in the DPC 2012 Annual Report:

*Those recommendations which were not implemented by FB-I as of [the date of the 2012 Audit Report] were highlighted with a clear timescale for implementation listed. A deadline of 4 weeks for those matters to be brought to a satisfactory conclusion was set and FB-I progressed those matters to our satisfaction within the four week period.<sup>14</sup>*

## **4.5. Partner Categories**

The Complainant alleges that FB-I is seeking to build “shadow profiles” via “co-operation with data brokers”<sup>15</sup>. This appears to be a reference to FB-I’s Partner Categories.

At present, Partner Categories is only offered by Facebook, Inc., and not FB-I. Partner Categories is only available to US advertisers and is designed to target advertising to individuals in the US, based on the US records held by Facebook, Inc.’s partners. Consequently, this technology is not relevant here. For the sake of completeness, however, it should be noted that Facebook, Inc. and its partners use hashing and similar technologies to ensure that Facebook, Inc. does not obtain any additional personal data of its users as a result of Partner Categories. Like FBX, Partner Categories has been built from the ground up with privacy considerations, such as data minimisation, in mind.

## **4.6. Publicly available data**

The Complainant asserts that FB-I is using publicly available data, including data from Wikipedia, to build “shadow profiles” of its users.

This assertion is unfounded. FB-I does not supplement users’ accounts with data collected from Wikipedia or other publicly available internet sources.

## **5. APPLICATION TO CURRENT COMPLAINT**

---

<sup>13</sup> Page 28 of the 2012 Audit Report

<sup>14</sup> Page 19 of the Annual Report of the Data Protection Commissioner 2012

<sup>15</sup> Page 40 of the Request for Formal Decision

In light of the above, FB-I would respond to the specific factual allegations of the Complainant as follows:

(a) *FB-I creates “shadow profiles” of its users and non-users.*

This assertion is simply wrong as shown by the DPC during the audit.

(b) *FB-I uses social plugins to build “shadow profiles” of both users and non-users.*

This allegation was investigated and dismissed by the DPC during the audit.

(c) *FB-I scans message content to build “shadow profiles” of its users.*

This allegation was investigated and dismissed by the DPC during the audit.

(d) *FB-I uses synchronised and imported contacts to build “shadow profiles” of its users.*

This allegation was investigated and dismissed by the DPC during the audit.

(e) *FB-I uses inferred profile completion questions to build “shadow profiles”.*

FB-I generates timeline completion questions in real time. FB-I caches suggestions for limited periods of time and, as the DPC confirmed, such suggestions are not influenced by the content of messages.

(f) *It is possible for a user who creates a new profile to infer the friends list of another user, even if that latter user has hidden their friends list.*

FB-I fails to see what this has to do with alleged “shadow profiles”. The Data Use Policy informs users that while they can control the visibility of their friends list on their timeline, their friends list may be visible elsewhere on the site.

(g) *FB-I is using content provided by other users about their friends to build “shadow profiles”.*

Facebook is a social network, based on sharing content and information. Given the social nature of the platform, Facebook users can involve their friends in their posts. It is possible for users to provide content about their friends, such as by tagging them. Where this content is associated with the friend, it is made accessible to that friend in the same way as other tagged content.

(h) *FB-I is using Facebook Exchange to build “shadow profiles”.*

Facebook Exchange was subject to technical investigation by the DPC during the 2012 audit. The DPC’s expert noted that this technology limited the flow of information to FB-I and the DPC expressed no concerns that this was being used to create “shadow profiles”.

(i) *FB-I is using Partner Categories to build “shadow profiles”.*

Partner Categories is only offered by Facebook, Inc. in the United States and is not available in the EU. For the avoidance of doubt, Partner Categories contains a number of privacy safeguards and is not used to build “shadow profiles”.

(j) *FB-I is using publicly available information, particularly that taken from Wikipedia, to build “shadow profiles”.*

This allegation is not correct. For the avoidance of doubt, FB-I does not use publicly available information to build “shadow profiles” of its users.