Office of the Data Protection Commissioner.
Canal House, Station Road
Portarlington , Co. Laois
IRELAND

[redacted]
AUSTRIA

Vienna, 19th of September 2011

Complaint against Facebook Ireland Ltd. – 19 "Pictures Privacy Settings"

To whom it may concern,

This is a formal complaint against "Facebook Ireland Ltd." under section 10 of the Irish DPA. I am convinced that "Facebook Ireland Ltd." breaches the Irish DPA and the underlying Directive 95/46/EG and I kindly ask you to investigate the following complaint.

I am a user of "facebook.com". The contract is governed by the "terms" used by Facebook (attachment 01). They state in section 18.1. that all users that live outside of the United States of America or Canada, have a contract with Facebook Ireland, while all users within the United States of America and Canada have a contract with Facebook Inc., based in California, United States of America (further called "Facebook USA").

Therefore I do have a contract with "Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2, Ireland" (further on called "Facebook Ireland"). For preforming my contract with them, Facebook Ireland is processing my personal data in different means. Since this controller is established in Ireland, I understand that according to section 3B(a)(i) DPA the Irish Data Protection Act (DPA) applies.

Because facebook.com is similar to a "cloud" service, I want to distinguish between the mere "hosting" of my data and all further processing of my data. For the purpose of hosting my data I see Facebook Ireland as a processor and myself as the controller. For any form of further processing of my data for Facebook Ireland's own purposes (e.g. analytics or advertisement) I see Facebook Ireland as the sole controller (see graphic in attachment 02).
Generally all my hosted personal data is also used for Facebook Ireland's purposes, which is why Facebook Ireland must always be seen as a controller. Whenever Facebook Ireland processes data that was "removed" by the user, it is obvious that the user is not in control of the data; therefore Facebook Ireland is the sole controller at this time. Facebook USA must be seen as the sub-processor or the processor in each case.

Unfortunately Facebook Ireland does not have a certain structure in its processing that would make it easy to distinguish certain forms of processing. In order to make the handling of my complaints easier for you, I decided to split them into individual cases. I want to inform you that some cases are overlapping to a certain extent.

Complaint 19: "Picture Privacy Settings"

Facebook Ireland Ltd. gives all users the possibility to upload pictures that are then hosted on facebook.com and also processed by Facebook Ireland Ltd. for its own purposes. All users are given the option to choose specific "privacy setting". The options are "public", "friends of friends", "friends only" and "only me", as well as customized lists of users.

Facebook Ireland is heavily promoting these options and makes users believe that only the chosen circle of people can access the pictures that were uploaded (see attachment 03).

After reading the source code of the picture pages of facebook.com we easily found out that all URLs of pictures stared with "http://fbcdn-sphotos-a.akamaihd.net/hphotos-ak" and were followed by numbers, of which a part was the (public) UserID of the Facebook user. The URL is registered with "Akamai Technologies Inc." situated at 8 Cambridge Center, Cambridge, MA 02142, USA (see attachment 04). This means that Facebook Ireland Ltd. has outsourced the delivery of the content to "Akamai Technologies" as a "Content Delivery Network". From a legal standpoint this company is a processor that is bound by privacy laws. All actions of "Akamai Technologies" are undertaken on behalf of Facebook Ireland Ltd.

To our surprise, the picture were accessible at the URL despite privacy settings that should prevent this from happening. This means that anyone that was ever able to see the URL has potential access to the pictures.
After little research online we could also find guides on how to find (embarrassing) pictures that people have removed or hidden form a specific user on facebook.com (see attachment 05).

This means that Facebook Ireland is not really having a proper access management system but is only "hiding" links to pictures that are public on the internet. The URL mostly consists of consecutive numbers and the (public) UserID. Only the last couple of numbers seem to be random numbers that may protect the content against "brute force" attacks (see a list of URLs in attachment 06). Even the most basic webservers have a system that does not only "hide" links but actually limits the access to the content itself.

In a recent update Facebook also promoted the "new privacy settings" that include the option to change privacy settings after posting a piece of information (see attachment 03):

> *Change Your Mind After You Post?*
> *Before: Once you posted a status update, you couldn't change who could see it.*
> *Going Forward: Now you'll be able to change who can see any post after the fact. If you accidentally posted something to the wrong group, or changed your mind, you can adjust it with the inline control at any time."*

In fact only the link is hidden form the users, but not the content. Users that have accessed the picture before can find the link in the cache of a web browser and still access the link directly.

I do think this processing by Facebook Ireland is illegitimate under the Irish Data Protection Act and the Directive 95/46/EG for the following reasons:

1. There is no transparent notice that users can only control the links, not the actual content. The user is told that only a certain group of people can "access" the data while in fact anyone can access it. This breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EG.

2. There is no information in Facebook Ireland's privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EG. This constitutes another breach of the principle of fairness in Section 2(1)(a) DPA.

3. It seems that there has never been an informed consent to this form of processing, since the user just agreed to the processing by having the option limit the access at any given time. If Facebook Ireland does not really limit the access to the content but only the access to the link, the consent seems to be neither informed nor unambiguous and therefore void under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EG.

I therefore kindly ask you to take the necessary steps to change this illegal practice by Facebook Ireland and make Facebook Ireland comply with Irish and European law.
I think that this could only be achieved if Facebook Ireland sets up contractual and technical measures to ensure that the content delivery networks limit the access in the very moment that the settings are changed on facebook.com.

It seems very likely that Facebook Ireland's systems for other content (e.g. videos) follow the same general rules so that I would encourage the DPC to investigate all other forms of content delivery by a third party as well.

I decided to only send you the relevant parts of the original documents as attachments to this complaint. All original files can be sent any time by airmail, if necessary. I can be reached at [redacted] f you have any further questions.

Sincerely,

[redacted]