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

[redacted]
AUSTRIA

Vienna, 18th of August 2011

Complaint against Facebook Ireland Ltd. – 13 "Applications"

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.

Case 13 – Applications

Facebook Ireland offers all its users the option to use third party "applications" on facebook.com. These applications are developed, managed and run by third party companies that can be situated anywhere in the world. The applications run on external systems but Facebook Ireland allows the providers of the applications access to the data it is hosting. According to Facebook Ireland's statistics page there are more than 20 million applications installed by users every day.

This constitutes a tremendous threat to data privacy on facebook.com. There are only very limited contractual measures that Facebook Ireland is taking to ensure that developers of applications have an adequate level of data protection (see the yellow text in attachment 03).

There is no way that Facebook Ireland would be able to ensure real compliance with these limited contractual measures. The Wall Street Journal found out in October 2010 that *"all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies"* (see attachment 04).
Another example: Many applications do not even have a privacy policy, even though Facebook Ireland requires this. When I was checking on the 12 applications Facebook was randomly suggesting on my profile, 4 did not have a policy while 5 did have a policy right after I clicked on them (see attachment 05). Apparently Facebook Ireland is not even enforcing this very basic provision.
When the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy (see e.g. page 5 of attachment 05).

While Facebook USA is a member of the Safe Harbor Agreement, developers are not obliged to be a member of Safe Harbor. This means that Facebook Ireland is exporting personal data to other companies that do not have an adequate level of data protection, including companies in the USA which are not member of the Safe Harbor.

Most users are not aware that if a "friend" on facebook.com installs an application, the application can automatically access their profile picture, name and other basic information (see privacy policy in attachment 06). Note that Facebook Ireland is hiding this consent for the use of other users' data under the section "my basic information" (see e.g. page 4 in attachment 05)
If the person that is installing the application is consenting to it, the application can read all information about all friends that the person can see. Again this means that not the data subject but "friends" of the data subject are consenting to the use of personal data. Since an average facebook user has 130 friends, it is very likely that only one of the user's friends is installing some kind of spam- or phishing application and is consenting to the use of all data of the data subject. There are many applications that do not need to access the users' friends personal data (e.g. games, quizzes, apps that only post things on the user's page) but Facebook Ireland does not offer a more limited level of access than "all the basic information of all friends".

All this can only be prevented if the user turns off "platform" (opt-out). This can be done by clicking a button which is again well hidden (see attachment 07). There is no possibility to use applications without the possibility that other users can access the user's data (all or nothing). The data subject is not given an unambiguous consent to the processing of personal data by applications (no opt-in).
Even if a data subject is aware of this entire process, the data subject cannot foresee which application of which developer will be using which personal data in the future. Any form of consent can therefore never be specific.

Facebook Ireland could not answer me which applications have accessed my personal data and which of my friends have allowed them to do so. Therefore there is practically no way how I could ever find out if a developer of an application has misused data it got from Facebook Ireland in some way.

I 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 has never been an informed specific and unambiguous consent, by the data subject to the use of personal data. All processing of third party data is therefore illegitimate under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EG.

2. There is only limited information in Facebook Ireland's privacy policy. The consent to the use of friend's information is hidden under the section "my basic information". Accurate information is needed to comply with section 2D DPA and Article 10 of Directive 95/46/EG. This constitutes a breach of the principle of fairness in Section 2(1)(a) of the DPA.

3. There seems to be a breach of the principle of purpose-based processing. The user shares personal data for the use on facebook.com but not for another purpose of some third party "application". This breaches section 2(1)(c)(i) DPA and Article 6(1)(a) of Directive 95/46/EG.

4. The possibility of developers to access personal and potentially sensitive data without any prior checking by Facebook Ireland and very limited enforcement of the most basic provisions cannot be seen as processing with appropriate security measures as necessary under section 2(1)(d) DPA and Article 17 of Directive 95/46/EG.

5. Facebook Ireland does not ensure in any way that the developers of applications ensure an adequate level of protection for the privacy and fundamental rights and freedoms of the data subjects as necessary under section 11 DPA and Article 25 of Directive 95/46/EG.
   Consent of the data subjects to the transfer is unlikely since many applications do not have a policy that would explain to which county the data is flowing and the actual data subject is not even asked.

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 applications can only be used if they are only processing the user's own data. There might be exceptions when the other data subject's information is only used for private or household activities (such as downloading information to a mobile phone). There should be appropriate data protection measures with a proper form of enforcement. Developers have to be within the EU or members of the Safe Harbor agreement.

I can be reached at [redacted] or [redacted] f you have any further questions.

Sincerely,

[redacted]