facebook

March 9th 2012

Dear Max:

We write to respond to the follow-up questions you pose in your "Summary of Arguments". To begin with, however, we comment on two general points in your Summary of Arguments.

First, your Summary reflects that you do not agree that Facebook Ireland Ltd (FB-I) is the "data controller" under the Data Protection Acts, 1988 and 2003, which give effect to the European Union's Data Protection Directive 95/46/EC ("the Acts"), with respect to much data that FB-I receives from users. However, as the Office of the Data Protection Commissioner of Ireland (ODPC) described in its Report of Audit ("Audit") of Facebook Ireland Ltd (FB-I), FB-I is the data controller with respect to European users' data, and FB-I has a robust operations – employing over 400 individuals – carrying out the duties of a data controller. The Audit examined all aspects of FB-I's compliance with the Acts as a data controller and made recommendations for FB-I to enhance its practices and policies. FB-I agreed to follow most of the ODPC's recommendations and to consider seriously the rest. As a data controller in Ireland, FB-I submits to the jurisdiction of the ODPC and is committed to complying fully with the Acts. FB-I contracts with Facebook Inc., to host the Facebook service and to process data on FB-I's behalf. Irrespective of FB-I's obligations as a data controller, FB-I provides users with significant granular control over the data they add to their timelines (formerly, profiles). We consider this a resolved issue.

Second, you state that FB-I "needs to stick to the legal definition of consent". FB-I obtains the (1) unambiguous, (2) freely given, (3) specific, and (4) informed consent, which is not obtained by deception or misrepresentation, of our users upon their registration and agreement to our Data Use Policy and Statement of Rights and Responsibilities. Our Data Use Policy provides a comprehensive, easy-to-read and understand description of the data FB-I collects and how it is used. FB-I provides easy-to-access (drop-down from "Home") and granular privacy and account controls for users to manage the visibility and sharing of their data as well as other settings in their accounts. When FB-I makes material revisions to its Data Use Policy, it provides a notice and comment period for users to review the new provisions and comment if they like. FB-I's governance policy in fact contemplates that if it receives enough comments, the policy provisions at issue will be put up for a vote. We know of no other web service that has such a policy of seeking input from its users. After having reviewed the revisions, the user's continued use of the Facebook service is deemed consent to the revised terms. Furthermore, as part of our commitments to the Irish DPC following the audit, FB-I will be making enhancements to the new user registration process to give new users more information about our privacy control tools. We consider our commitments to resolve this concern.

Third, you continue to maintain that the information FB-I holds of non-users is a "shadow profile". The ODPC did an exhaustive technical examination of our databases and code and established that we do not create any such semblance of a "shadow profile." We consider this a resolved issue.

facebook

We now turn to your follow-up questions:

First, you asked for which purposes "pokes" are retained and how long Facebook retains them. Like many actions users take on Facebook, the poke is another piece of data that we may use to provide the Facebook service. In the Data Use Policy, we are clear that we receive data when the user interacts with the Facebook service: "We receive data about you whenever you interact with Facebook, such as when you look at another person's profile, send someone a message, search for a friend or a Page, click on an advert or purchase Facebook Credits." We are also clear that we use the data we receive in connection with providing the Facebook service:

> We use the information we receive about you in connection with the services and features we provide to you and other users, such as your friends, the advertisers that purchase adverts on the site and the developers that build the games, applications and websites you use. For example, we may use the information we receive about you:
>
> - as part of our efforts to keep Facebook safe and secure;
> - to provide you with location features and services, like telling you and your friends when something is going on nearby;
> - to measure or understand the effectiveness of adverts that you and others see;
> - to make suggestions to you and other users on Facebook, such as suggesting that your friends use our contact importer because you have found friends using it, suggesting that another user add you as a friend because the user has imported the same email address as you or suggesting that your friend tag you in a picture they have uploaded with you in it.

We have previously told you that one of the purposes of saving poke data is to be able to determine if user harassment has occurred. As described above, we may use poke data for other purposes in connection with bringing the Facebook service to users. Most of the data that we receive from user actions on the site will be retained until the user deletes his or her account. As part of our commitments following the audit by the Irish Data Protection Commissioner, we are going to make certain data, where feasible, able to be deleted on a per-item basis.

However, it should be understood that the value of the Facebook services rests in the positive engagement users experience on Facebook. We make use of the data users provide and that we receive to make our users' engagement better. Facebook uses proprietary algorithms to determine the best content to surface in the user's news stream, possible friends to suggest, and the most relevant ads to serve. In other words, our processing of user data is in the interests of our users, and, if data such as pokes or any other actions a user takes on the site serve to better inform our algorithms and to improve the user's experience, we may make use of such data. We consider the many commitments that we made regarding data deletion and retention policies and practices to resolve this issue.

Second, you questioned whether Facebook would give the user the option of deleting the record of a removed tag. We do not at this time have any plans to do so given that our means of preventing a user from being re-tagged is the data of the removed tag. We have sufficient legitimate reason to

retain data regarding the un-tagging action in order to provide our users with the experience they are expecting, which is not to be re-tagged. We consider this a resolved issue.

Third, you asked whether there was a change in the amount of information that Facebook receives when a user syncs the iPhone with Facebook. Facebook receives the contact information in the iPhone contacts list, which may include: name, phone number, and email address. All of the synced data can be found by the user in his or her address book on Facebook and can be deleted in its entirety. We consider this to be a resolved issue.

Fourth, you asked what the purpose of giving Facebook apps the right to access certain data, e.g., text messages. We assume you are referring to the read/write permission sought by the Facebook app on the Android phone. This permission was sought for a specific feature that we planned to implement but did not. Facebook does not access users' text messages on their phones. We do not consider that there is an open issue regarding this concern.

Fifth, you asked whether posts that the user deletes are actually deleted, and, if so, how the deletion process works. Our policy is to remove the post as soon as the user deletes it, and to begin the process of deletion within 14 days, and to have the post removed from our servers within 90 days of deletion. Back-up copies may reside in inaccessible places longer than that period. The Audit details the complexity of our storage system and concludes that the above policy meets our obligations under the Acts. We consider this to be a resolved issue.

Sixth, you asked whether the "traffic data" related to messages on Facebook were used and if so for what purposes. FB-I does not use traffic data. We do not see an open issue here.

Seventh, you asked for a list of the categories of personal data that we hold of users. We attach the list to the end of this letter. As agreed to with the ODPC, Facebook is working to make all such data available in a self-service format. Given the technical challenges of this, it will be done on an incremental basis. The ODPC performed an exhaustive review of the personal data that FB-I holds of users and thoroughly examined any potential reasons for withholding any data. The ODPC determined that only in rare circumstances would FB-I have a legitimate justification for not providing a certain category of data to users upon request. FB-I therefore committed to making all of the data available that the ODPC determined it was legally obligated to provide. Furthermore, FB-I discloses in its Data Use Policy all of the data that it collects and receives from users and the purposes to which the data is put. FB-I has also committed to enhancing the disclosures in the Data Use Policy where the ODPC found more details would be helpful. We consider this issue therefore resolved.

Eighth, you asked whether FB-I used social plugin impression logs for any other purposes than what we stated in our meeting. The intended purposes for retaining the impression data for a period of 90 days are for the security and performance activities that we described. Following our normal practices, if there were any substantive new uses for this or any other data then we would make our users aware, such as through our Data Use Policy. We are unclear about your second question regarding Page views. Logs are created for actions users take on Facebook, including Pages visited.

facebook

We consider the issues of the use of social plugin impression data and the retention period for such data to be resolved.

And ninth, you asked about whether FB-I has a contract with an EU subsidiary of Akamai USA. FB-I has an agreement with Akamai that requires Akamai to comply with the Safe Harbor requirements applicable to it as a processor of user data. We do not see an open issue here.

FB-I agreed with the ODPC to numerous enhancements to its data protection and privacy practices and policies, many of which specifically address the concerns articulated in your complaints. We urge you, therefore, to reserve further complaints for after July 2012, when the ODPC will audit FB-I on its implementation of its commitments.

Best Regards,

Richard Allan
Director of Policy EMEA
Facebook