

June 11, 2009

Director Janni Christoffersen  
Danish Data Protection Agency  
Borgergade 28,5.  
DK-1300 Copenhagen, Denmark

A Internet  
F  
- 1 JULI 2009  
J.NR.  
Bilag

Dear Ms. Christoffersen:

Thank you for your letter of April 3, 2009 inquiring about Facebook's privacy practices.

At the outset, we note that Facebook and the Danish Data Protection Agency share a common goal of providing users with a safe and privacy protective on line environment, as well as respect for the user control principles reflected in European and Danish privacy law. Accordingly, we look forward to working with you as we have with regulators around the world, and we are pleased to provide the following response.

Facebook's practices with respect to user data are explained in detail in our Privacy Policy, posted on the Web at <http://www.facebook.com/policy.php>. This document is available in a number of languages including Danish. In addition, the following comments are consistent with the remarks that Mozelle Thompson and I have made in various fora, including meetings of the Berlin Working Group and the International Data Protection Commissioners Conference in Strasbourg last fall.

### **Deletion of Accounts**

You have asked what user options are available to delete accounts on Facebook. Facebook offers users the option of either deactivating their account or deleting it entirely. You can deactivate your account from the Account Settings page, accessible from the top right of any Facebook page. When you deactivate, your profile and all information associated with it are immediately made inaccessible to other Facebook users. If you want to reactivate your account at some point, you can do this by logging in to Facebook again with the correct email address and password combination. Many users deactivate their accounts for temporary reasons and expect their information to be there when they return to the service. People who know they do not want to use Facebook again can delete their accounts through the form we provide on our Help page. Deleting your account scrubs personally identifiable data elements like name, birth date, and contact information from our servers. This means that the account cannot be reactivated or reconstructed.

You indicate in the letter that some users may be having problems using our procedures for deletion. We have received some reports from users who have seen an error message telling them they have the wrong email and password combination when they try to delete their account through this form. We are investigating this issue, but so far are unable to reproduce it. We believe the problem may reflect either a browser issue, or an incompatibility between the captchas (words in a box) we show and certain foreign

**facebook**

Address: 1601 S. California Avenue  
Palo Alto, California 94304  
Telephone: 650.543.4800  
Fax: 650.543.4801

language keyboards. We will continue to look into this, and would like to discuss this problem with you further.

### **Deceased Users**

You have also asked about our procedures as to deceased users. When we receive a report that a user is deceased, either by email or through one of the many report links we provide on the site, we put that user's profile in a memorialized state. Certain more sensitive information like contact information and recent status update is hidden, and privacy is set so that only friends can see the profile and find the person in search. We do honor requests from close family members to either deactivate or delete the account entirely. We generally do not require any kind of special documentation for this, although we may do an independent investigation of the profile to confirm that the person is actually deceased before taking action.

### **Third Party Applications**

Additionally, you have asked for clarification on the data sharing with third parties that happens with the use of applications. When a user authorizes a third-party application, the user allows that application to request his or her Facebook data. This data includes the user's interests, photos, videos, notes, groups and events joined, etc. (A more complete list can be found in the "Applications" section of the Privacy Settings page.) Applications are not given access to users' contact information. To ensure that users are aware of this information sharing, Facebook gives users notice before allowing the user to connect to an application. This notice warns that the application gives the application access to the user's data and asks for consent to allow the connection.

Application providers' access to user information is also constrained by both technical and policy limitations. For example, application developers must have a confirmed Facebook account with a valid email address, and applications are prohibited from storing most Facebook user data for longer than 24 hours. Applications are also required to have and post their own privacy policy that lists the information they use and the purposes for which it is used. Users can also report applications they think are violating our data policies through a report link on the application's "About" page, or by writing an email to our support staff. In addition to technological tools we use to determine whether an application might be violating these policies, Facebook employs a team to review applications that have either been reported by users or flagged by one of our own automated systems. When we find that an application is misusing data, we warn the developer or disable the application completely. To date, Facebook has disabled more than 1,000 applications deployed on Facebook Platform.

Our practices around sharing information with third parties more generally are explained in our Privacy Policy. We are additionally required to provide information to law enforcement when we receive a valid subpoena or court order. We only do this, however, when we have a good faith belief that the request meets applicable legal standards.

## **Monitoring and Retention**

You have also asked about our policies with regard to monitoring activity and communication on Facebook and our approach to data retention. Facebook generally believes that users should have the freedom to express their thoughts and ideas on the site, but has developed several automated systems that detect anomalous site activity for the purpose of maintaining Facebook's safe and trusted environment. These systems are used, for example, to protect users under 18 from inappropriate contact by adults. They are also employed to flag users who are sending lots of messages to non-friends, for example, or whose friend requests are being ignored at a high rate. They also block links to known malicious websites to help protect the security of users' accounts. When a user deletes public content from Facebook, such as a Wall post, it is immediately made inaccessible through the service and the space made available to be overwritten. Backup copies may exist, however, for a short period of time in order to ensure that the account is not being deleted to hide evidence of criminal activity. Private messages sent between two or more Facebook users, however, generally cannot be deleted. Although they may be removed from the Inbox of the requesting user, it will still exist in the Inboxes of others who sent or received the message. This is similar to how email works.

## **Jurisdiction**

Facebook is not established as a data controller in the European Community, nor do we have any equipment in Denmark. We do collect information from Danish citizens for processing in the United States, and for this we gain the consent of users through their voluntary acceptance of the site's Statement of Rights and Responsibilities and Privacy Policy. We also participate in the US/EU Safe Harbor Privacy Framework as set forth by the US Department of Commerce.

While Facebook is not a data controller, it aims to act in all instances with the respect that a data controller is expected to show to an individual's personal data. Facebook's extensive privacy controls are designed to give users the power to share as much or as little as they want, with the people they choose.

We understand that the Article 29 group has suggested a position that would subject companies to direct jurisdiction in European countries based merely on the placement of a cookie on a user's machine. We believe this interpretation of jurisdiction is dangerously overbroad and is inconsistent with the longstanding Safe Harbor Agreement between the US and EU, which was designed to provide a mechanism for US companies to respect the personal data of European citizens while insuring the free flow of information across the Atlantic.

Facebook affirmed its respect for those principles in 2006, very early in its existence, and continues to operate within the spirit of European privacy law by constantly refining and improving the technical tools it gives users to exercise control over their personal data.

As a site with over two million active Danish users, we appreciate the opportunity to continue our dialogue with you, and look forward to future collaboration. Please let me know if you have further questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Chris Kelly', with a long horizontal flourish extending to the right.

Chris Kelly  
Chief Privacy Officer  
Facebook