facebook

Answers to the questions on the Collection and Use of Personal Information by Facebook

1) **Data collection in relation to the "Like" button and cookies, particularly the datr cookie:**
   - **What data is collected from Facebook users who are logged in** if they visit a page which has the Facebook button integrated and this is not clicked? How long, in what form and for what purpose is the information about the visited page stored? Does this information remain assigned to the user account and therefore to the user's name for 90 days? Is the data anonymized at any time and, if so, in what way and after how long?

Attached (Like-Button Scenarios DE) you will find an overview of what is stored when visiting a page with a Like button (please note the comments at the end of the page). The information about a visit to a page is stored for 90 days. After 90 days, it is anonymized and stored in aggregate form (with no link to the profile). We are using this data to improve our performance of plugins and on our site.

The report of the Irish data protection authority published on December 21 also contains a passage about this. This reads:

"Tests were also performed to attempt to establish whether or not the act of a logged-in Facebook user simply browsing to pages that have social plugins (as opposed to clicking the "Like" button) would influence the advertising that the user is presented with. An affirmative result would strongly indicate that Facebook were using browsing activity to target advertising, which it is claimed is not the case.
No correlation with browsing activity was identified."

   - **Which data is collected from users not logged in and from non-members,** and is this stored in grouped form? Which cookies are used to store the data? Are non-members informed of this data collection and is there an option to refuse this? Is the collected information assigned to the user when logging in to Facebook or when creating a Facebook account? Theoretically, would such an assignment be possible? If so, why is the possibility of assignment not technically excluded?

I would like to refer you to the enclosed overview again here. This data is not stored using a cookie. A datr cookie is only used if someone has already visited facebook.com — not when visiting a webpage with a social plugin from Facebook. In addition, the data we obtain using a possible datr cookie is stored briefly for just 10 days instead of 90 days. Therefore, (even if we wanted to) the data cannot be used for creating profiles and also cannot be subsequently assigned to any newly created account.

I would also like to refer you here to the results of the audit by the Irish data protection authority in relation to this. This states:

„As outlined in the technical analysis report, this Office is satisfied that while certain data which could be used to build what we have seen termed as a "shadow profile" of a non-user was received by Facebook, no actual use of this nature was made of such data and as outlined elsewhere in this report, Facebook is now taking active steps to delete any such information very quickly after it is received.
We are satisfied that FB-I does not use or seek to use any information that might identify a person who has never visited Facebook that it may have collected inadvertently via the social plug-in. "

In addition, we have agreed the following with the Irish authority, as discussed:

„It is accepted by all that it is not appropriate for Facebook to hold such information other than for a very short period for very limited purposes. FB-I has therefore undertaken to implement what it has termed an aggressive retention policy. Under the new policy, when either a person who has never visited Facebook.com or a person who has visited Facebook.com but is not logged in to the service then visits a site with a social plugin and does not log in or register with Facebook, FB-I will immediately anonymize the IP address by dropping the last octet when it is logged; FB-I will delete the browser cookie that is recorded from its servers within 10 days; and FB-I will delete the anonymized logs from its servers after 90 days. This approach allows FB-I to retain information about social plugins to identify and resolve any technical issues in the operation of the service, and then eliminate it once FB-I does not need it for those purposes."

Furthermore, I would like to refer you to our (publicly available) letter to the ULD (also enclosed) in which we also address these points.

- **Why is a cookie that is valid for almost two years used,** even though the data collected with this is supposedly deleted after 90 days?

This is related to security issues. To answer your questions about the use of cookies, I would like to refer you to an article from Spiegel Online:
http://www.spiegel.de/netzwelt/netzpolitik/0,1518,799909,00.html
(and also enclosed). This contains a wealth of information, which also shows that the datr cookie performs several functions which justify its longer storage time.

- **Is Facebook considering offering a "two-click button"** which only activates the actual data transfer (2nd click) after receiving information about the intended data transfer (1st click)?

In our view, the "two-click solution" for the "Like" button is not a suitable solution, which is why we do not actively support it. Instead, we intend to find a solution that supports the simple version of the button. As we understand it, we already have a data protection-compliant solution because, as can be seen from the aforementioned enclosure and has been outlined several times, no personal information is stored using the "Like" button. We are also communicating with the data protection

authorities about this.

Moreover, I would like to point out that this discussion must ultimately be conducted independently of the "'Like' button" issue. The integration of content from third-party providers via iFrames is now common on virtually every website. Facebook is no different from other providers in this respect. The display of advertising, cards, music and tickers, for example are functions according to exactly the same principle. The discussion should therefore address the question of whether and how the Internet of today can be structured in a data protection-compliant way.

- **Does Facebook want to provide clearer information in the future about the transfer and use of data?**

We continually strive to be better. This also applies to the subject of information for people on Facebook.

Again, here I would like to refer you briefly to the report of the Irish data protection authority, which shows that we have agreed to cooperate with ***the DPC in order to provide people who use Facebook with better information regarding the control of their data. This should apply to both Facebook and applications used on Facebook.***

2) Facial recognition:

- **Which pictures are biometrically recorded?** In particular, apart from tagged pictures, are profile pictures also used for this? Is it correct that only "friends" can be tagged? Was the tag suggestions function able to access a set of pictures when the function started? If so, which pictures?

First of all, we would like to clarify how the "Tag Suggest" feature operates. Facial recognition software is an algorithm that is passed over an image of a face and calculates a unique number (hereinafter "template") based on distinguishing characteristics, such as the shape of the eyes, and the distance between eyes, nose, and ears. Once the template is calculated, you can pass a new image to the algorithm, have it convert that to a number, and compare if the number matches any existing templates.

The Template is created based only on pictures in which a person was tagged and has not rejected the tag are used. Furthermore, Facebook user is suggested only the names of friends from his or her closest circle of friends to tag in an uploaded photo, if there is a match. This means that it is not possible to upload a photo to Facebook and identify unknown people in it (as you addressed in our conversation). The tag suggestions function has not accessed any existing tagged pictures; the recording of biometric features only began once the function was activated. If the function is deactivated by a user, all biometric data is deleted.

- **Are tagged pictures biometrically evaluated before the tagged person has approved the**

tag? Which information does Facebook collect if someone does not respond to the notification that he or she has been tagged? Are these pictures also biometrically recorded? What are the consequences of rejecting a tag? What are the effects of this rejection on recorded biometric data? Is biometric information obtained from a tagged picture deleted if the tag is rejected?

Users are notified each time they get tagged in a picture. They consequently get more control over the content and get the opportunity to untag themselves. If a user decides to remove the tag, the picture will not be used for the creation of the Template.

Users get ***the ability to opt-in for the tag review feature, which allows them to preapprove tags before they appear on their Timelines (formerly, profiles). If a user decides to simply block the picture from appearing on his own Timeline, but does not untag himself, then the picture*** *will be used for the creation of the template.*

To conclude, only tagged photographs are used to create the template that provides the suggestion function. Until a user removes a tag, that tagged photograph can be used to add to the template.

- **What are the consequences of deactivating tag suggestions?** Does this result in the complete deletion of all existing biometric data about the person in question from all Facebook databases? Does deactivating tag suggestions also result in no further biometric data being recorded when pictures of the person in question are tagged in future?

The deactivation of the tag suggestion function causes all existing biometric data to be deleted and no further biometric data to be collected.

- **What is the difference between deactivating the tag suggestions and the method** for deleting biometric data using the help function?

By contacting the Photos team, users can indicate that they want to be permanently opted-out of ever having a template created again in the future with regard to other products, tools, or features that may have use for facial recognition technology.

Disabling Tag Suggest is a feature-specific opt-out. ***It results in the deletion of the photo-comparison data that we use to make Tag Suggest work.***

- **Which part of the biometric database is searched to provide a tag suggestion** if someone uploads a picture? Only pictures of friends or the entire database? Is further information obtained from this matching process? Is it possible that Facebook will use a broader basis for matching uploaded photos at a later date?

Currently, tag suggestions are only made of a users' closest circle of friends. We do not have any

immediate plans to expand the feature.

- **Is information also stored if someone rejects a suggested tag?** If so, which information?

Suggestions are just that: suggestions. If a user does not take a suggestion, then no tag is made and no record is kept.

- **Why can the tagging option not be deactivated?**

Tagging as such and the tag suggestion function must be differentiated. Tagging is an important tool for users to control their own data. Deactivating this would only be disadvantageous for users as, for example, you would no longer be informed if your name appeared in relation to a picture and you would not be able to intervene.

3) **Data collection during synchronization:**

- **For what purposes are the telephone numbers collected when synchronizing smartphones used?** In particular: Are these used to analyze who knows whom?

The synchronisation is an optional service that allows users to back up their mobile contact details. Users may subsequently choose to issue friend requests to uploaded contacts or not.

- **How does Facebook inform users** about which information is collected in the Friend Finder and when synchronizing smartphones and how this information is used?

We inform our users in the section "some other things you need to know" of our Data Use Policy that: „We offer tools to help you upload your friends' contact information so that you can find your friends on Facebook and invite friends who do not use Facebook to join. If you do not want us to store this information, visit this help page. If you give us your password, we will delete it after you upload your friends' contact information."

- **Is Facebook considering allowing users to choose to synchronize their email contacts only** without making telephone numbers accessible? Is Facebook considering allowing users to transfer contacts individually?

No, we do not plan to implement these changes in the near future.

- **What options do people who do not use Facebook themselves** have with regard to having their telephone numbers, email addresses or other information **deleted from Facebook**?

As already explained verbally, both telephone numbers and email addresses of users are used to suggest friends. However, all such data can be deleted via the Help Center. All contacts uploaded and invitations sent can be removed:

https://www.facebook.com/invite_history.php
https://www.facebook.com/contact_importer/remove_uploads.php

Incidentally, the functions of the Friend Finder were revised in cooperation with the Hamburg data protection authority. The proceedings initiated against Facebook were dropped by the authority in summer 2011.

4) Facebook's security precautions:

- **What security precautions** does Facebook implement to prevent a password being guessed or other ways that an account may be hacked? Are such security precautions limited to automated attacks?
- **Are there security precautions for preventing someone from trying to log in to multiple accounts within a short period of time?** If so, under what circumstances do these come into effect?

We provide a range of base security features by default on all accounts and monitor for suspicious activity on user accounts. Detection of suspicious activity will lead to additional authentication steps such as the user needing to fill out a CAPTCHA or by an SMS authorization code sent to the user's mobile phone.

We also provide a selection of opt-in security features, accessible under Account Settings->Security. They are:

- *Secure Browsing*
- *Login Notifications*
- *Login Approvals*
- *Active Sessions*
- *One-time Passwords*

Secure browsing enables the use of encrypted communication using HTTPS whenever possible. Secure browsing is not supported on the mobile platform. It has been confirmed that enabling secure browsing appears to causes all subsequent web browsing to be performed over HTTPS.

Login notifications involves notifying the user whenever their account is accessed from a computer or mobile device that has not been used before. Login approval involves entering a security code, which is sent to the user by SMS, each time the user's account is accessed from a computer or mobile device that has not been used before. It has been confirmed that enabling login notifications causes an SMS containing an authorization code to be delivered whenever a login is attempted from a web browser from which the Facebook user has not logged in before. It has also been confirmed that it does not appear to be possible to log in without the authorization code.

Active sessions allows a logged in user to see the locations from which their account is currently logged in and end activity from any particular session if that activity is unrecognized. It has been

confirmed that ending activity in active sessions immediately causes the relevant user session to be logged out.

One-time passwords is a feature to allow users protect their account when they log in from a public computer. The user sends an SMS to a particular number and they will receive an eight character temporary password, valid for 20 minutes, which can be used to access their account.

The availability of the one-time passwords feature appears to depend on country and mobile operator.

5) Youth protection

- Are there security precautions to prevent users from **logging in after specifying the incorrect age, even in a new online** session?
- Are there precautions to prevent **people who have an account as an adult** from logging in as a child with another account?

We have measures in place to prevent users from registering for an account with a fake age after initially failing with a correct, under-13 age. When a person attempts to register and enter a non authorized date of birth (i.e. under 13 years old) a „tooyoung" cookie is placed on his or her browser. If the same person attempts to register from the domain, the „tooyoung" will be sent to Facebook and the registration process will be blocked.

Furthermore, Facebook users are encouraged to report under users they notice on the platform. Our User Operation team disables accounts reported by users or detected through our security fraud model.

Finally, the use of real identity is a core value of the platform and highly contributes to the safety of our users. Under our Statement of Rights & Responsibilities, users agree to provide their real names and information, and to create only one account. We have developed technologies based on fraud model and also take action on tens of thousands of complaints each day from users who believe that another user on the site is inauthentic.

6) Timeline:

- **Why are users not permanently given the choice of whether** to display their profile as a "timeline" or keep it in its current layout? How can the encouragement to archive your entire life which is associated with the presentation of the new **layout** be reconciled with the **necessary sensitization of young people** to cautious use of their personal data?

Once Timeline is activated users have seven days to familiarize themselves with the timeline and adjust it to their personal comfort. The timeline is also a better product, which gives users much more control. Additional information on the Timeline and the benefits it brings to the users have already been submitted to you. Independently of this, we have a number of materials for young

people and also lots of information in the Help section on how to use Facebook safely (https://www.facebook.com/safety/groups/teens/)

7) Possibility of deactivating coverage analysis for operators of fan pages:

- Why does Facebook not give operators of fan pages (independently of the legal assessment) the option to refuse the storage of data about the use of their page?

For users in Europe, Facebook Ireland Ltd. is responsible for user data processing as the competent office. This also includes data processing via Facebook Insights. As described in the letter to Mr. Weichert, for example, this structure has been developed to ensure that administrators of Facebook pages do not have access to the personal data of Facebook users. As described in our data protection guidelines, Facebook uses data containing the data from Insights for its own purposes. We view usage data to determine which type of page contributions are positive and lead to higher user retention, and to identify the type of marketing measures to which our users respond; we also monitor the integrity and performance of the overall system in this way.

8) Facebook events:

- What proportion of the events organized in Germany using the Events tool is public and what proportion is private?

There is no separate data available for Germany. In general, however, more public than private events are created.

9) Data usage guidelines and consent to data usage:

The data protection page currently contains several questions, which you must click on individually and from which you are led to further questions via multiple menu levels, so what the consent refers to is unclear.

- Is there no longer an option to download or view the data protection declaration in full since the data protection declaration was restructured? If so, why does this option not exist in addition to displaying individual questions?
- The consent to the data usage guidelines is currently simulated with the registration on Facebook. Is there a change planned with regard to this, after which users will at least have to enable a check box in order to consent to a specific declaration stored here?

A downloadable version of the data usage provisions is planned and will be provided in the foreseeable future (it is already available in English). Moreover, we believe that the consent to our terms of use is effective.

10) Consent by friends and acquaintances:

Facebook collects and processes the data of third parties who do not use Facebook at different points. In addition, friends can approve information at several points (e.g. tags, addition to groups etc.) without the third parties in question having to expressly approve the information first.

- Does Facebook intend to adapt its service in this regard to European law, according to which those affected must consent to the use of their data themselves, and this consent cannot be replaced by the actions of third parties, even if these are friends? Is Facebook considering only storing the data of non-Facebook users in the Friend Finder if these third parties consent to this themselves (instead of the current option of rejecting this storage of data)?

We are confident that we are complying with European data protection law. As previously explained, tagging is an important control tool without which users would have much less control over what is said or written about them.

With regard to being added to groups, we have agreed on changes in the course of the audit with the Irish data protection authority. Firstly, we will revise the entry that appears in the News Feed if someone is added to a group in order to avoid giving the impression that someone has actually joined the group. In addition, who is invited to a group and who is already a "member" will be displayed in future.

"FB-I has also agreed to review and revise the news story that is created when a user's friend invites the user to join a group to avoid the suggestion that the user has in fact joined the group, until the user has been given an opportunity to leave the group. FB-I has also agreed to introduce a mechanism to identify, when viewing the group itself, which listed users are members, as compared to which users have merely been invited. The user status will change from "invited to the group" to "member" only after the user visits the group for the first time. The user will be able to check the content of the group and make a decision about whether or not he/she wants to be associated with this group. If a user does not want to be part of the group, he/she will be able to click on the option to leave the group."

With regard to information about the Friend Finder, as described above we have already devised improvements in cooperation with the Hamburg data protection authority at the start of 2011 which have been fully implemented and accepted by the authority.

11) Privacy by design:

- **Does Facebook implement precautions to secure the protection of privacy in the product in advance?** How many employees deal specifically with the task of data protection? Are suitable employees directly involved in product development? Are changes planned to improve the consideration of privacy protection in product development?

All products are also assessed with regard to data protection law and reviewed by data protection officials and others prior to being released.

A wide range of teams in our company deal with data protection matters (including the Legal department, security teams, Policy and User Operations). Hundreds of employees address these issues.

facebook

During product design, dozens of people deal with this subject, but we also obtain external advice and assistance: from outside counsels, privacy organization, data protection officials, our Safety Advisory Board etc. We also inform the Irish data protection authority about new products in good time. The authority can then express any reservations it may have, from which changes are derived where applicable. Our agreement with the FTC also states that we have appointed two highly qualified data protection experts to the roles of Chief Privacy Officer, Product (Michael Richter) and Chief Privacy Officer, Policy (Erin Egan). Michael Richter works on ensuring that the principles of user control, privacy design and transparency are consistently integrated during the product development process and in the products themselves. Erin Egan takes the lead in our commitment to global public discourse and the debate surrounding online privacy, while ensuring that feedback from regulators, legislative authorities, experts and academics from around the world is incorporated in all Facebook procedures and guidelines.