facebook

Dr. Thilo Weichert, Commissioner
Independent Centre for Privacy Protection for Schleswig-Holstein
Holstenstr. 98, 24103 Kiel, Germany

September 16, 2011

Re: Facebook's Detailed Response to Your Press Release of August 19, 2011, and Analysis of Facebook Services

Dear Dr. Weichert:

I write now to respond in some greater detail to the report published last month by the Independent Centre for Privacy Protection for Schleswig-Holstein ("ULD"). We found it very helpful that we could meet with your team last week to understand more about your concerns. We hope that the following information will be equally helpful to your team in understanding Facebook's services. We understand that you may put this response into the public domain.

As an initial matter, as we explained last week, Facebook Ireland Limited (Facebook Ireland) is the data controller for people using our service in Germany. Our European headquarters is not merely a "complaints handling service" as you described it in your report, but, rather, it is a substantial office with over 300 staff members. That number represents approximately 15% of Facebook's staff worldwide. The office carries out a wide range of functions to meet the needs of our users across Europe. This includes the determination of policies with respect to the processing of data of German users. This is a critical fact to be understood.

Furthermore, as your report correctly notes, Facebook's Hamburg office, Facebook Germany GmbH, is not involved in the processing of data of German users.

As a result of this structure, and of Art. 4 of Directive 95/46/EC and Sect. 1(5) of the German Federal Data Protection Act (BDSG), Facebook Ireland is subject to Irish data protection law. Facebook Ireland is not subject to the provisions of the German Telemedia Act (TMG).

We could dispute your position regarding applicable law and jurisdiction at greater length; however, we understand that the most pressing issues in your report relate to actions you propose to take against German organizations using our service. We therefore will not take the time to belabor our position with regard to applicable law and jurisdiction.

We will address the issue of Facebook Pages and Like buttons separately.

Pages

It seems to us that your preliminary conclusion that administrators of Pages may be in breach of the German TMG should be revised on the basis of the following points.

As we understand it, for the use of Facebook Pages by a person or legal entity in Schleswig-Holstein to be a violation of the TMG, three conditions would have to hold true.

First, the administrator of a Facebook Page would have to be regarded as being subject to the data protection provisions of the TMG (Sect. 11-15a). We believe that a Facebook Page administrator is not subject to the data protection provisions of the TMG.

Your view seems to be based on an assumption that administering a Facebook Page is similar to a commissioning a service from a web-hosting provider. It is not. A Facebook Page administrator is only able to carry out a very limited set of functions within a framework of rules defined by Facebook in our terms and conditions.

This limited set of functions does not include any that could be regarded as being a data controller for any user data on Facebook. Indeed, the structure has been designed to ensure that Facebook Page administrators do not have access to the personal data of Facebook users. Your report states that the ULD believes that Page administrators are responsible for the processing of personal data carried out when someone visits their Facebook Page. At the same time, your report appears to recognize that Page administrators do not actually do any processing of the personal data of users when it states that administrators cannot escape their obligation by using external service providers. In this way, your report suggests that Facebook processes personal data as a provider of services to the Page administrator. However, Page administrators, in fact, not only do not process user data, but they have no control or influence over the processing of usage data. Furthermore, there is no contract between Facebook and Page administrators for Facebook to process usage data on the administrators' behalf,[1] and there does not need to be any, because Facebook already has a direct contract with the Facebook user. Facebook uses the data that comprises Insights data for its own purposes, as described in our Privacy Policy. We look at usage data to determine what kinds of Page posts are positive and lead to more user engagement, and what kind of marketing messages our users are responsive to, as well as to monitor overall system health and performance.

Facebook Ireland is the data controller for the personal data of European Facebook users. The Facebook Page administrator can only be regarded as controlling the information that they choose to post on their Page; the administrator *is not* in control of any user data.

We understand that some German commentators have argued that the administrator of a Facebook Page may be required to provide certain information as required in Sect. 5 TMG (and Art. 5 of the E-Commerce-Directive 2000/31/EC). Even if this were correct, Facebook believes that this kind of obligation would not result in the Facebook Page administrator also being subject to the data protection provisions of the TMG, as these obligations are different in nature, define their applicability separately and have a different European law background (Directives 95/46/EC and 2002/58/EC instead of Directive 2000/31/EC). It should be noted that the model Facebook has created for Pages provides even greater privacy protection than if Page administrators were actual data controllers or processors and had to comply with the data protection obligations under the TMG. With the Facebook model, no personal data is provided to the Page administrator, and, therefore, there is no need for the protections under the TMG.

Second, under the terms of Sect. 12 and 15(1) TMG, the service provider would have to collect or process usage data. Facebook Page administrators have no ability to collect usage data of their Facebook

[1] The responsible entity as per Sect. 3(7) of the BDSG is the entity that "collects, processes or uses personal data for itself, or contracts with others to do so," or the entity as per Art. 2 Letter s) p. 1 of the EU-DSRL "that alone or with others makes decisions regarding the purpose and means of processing personal data."

Pages as described in Sect. 15(1) TMG. We have not seen it demonstrated in your Office's or any other report that Facebook Page administrators have access to such usage data as described in Sect. 15(1) TMG.

Third, under the terms of Sect. 15(3) TMG, the service provider would have to be creating pseudonymous user profiles. Facebook Page administrators have no ability to create such pseudonymous user profiles.

Facebook does not provide any such pseudonymous profile data to the administrators of Pages. In fact, no individual profile data whatsoever is provided to Page administrators, whether pseudonymous or identifiable. The only data that is provided to Page administrators are aggregate summaries based on Facebook's own analysis of data that it controls quite properly under the terms of its agreement with its users. We are therefore confident that any administrator of a Facebook Page in Germany can continue to administer their Page without breaching the terms of the German Telemedia Act (TMG).

Like Button

Turning to the analysis of the Like button in your report, we are concerned that this contains a number of incorrect assumptions about the ways in which Facebook uses data that is generated by user activity on third-party sites with Like buttons and stored in log files.

It is necessary to make a distinction between registered users of Facebook (in the following: Facebook users) and those individuals who are not Facebook users. Facebook Ireland obtains European Facebook users' consent for the use of their data associated with their use of the Like button through the Facebook Statement of Rights and Responsibilities and the Facebook Privacy Policy. We understand that your primary concern is not with Facebook users but with those individuals who browse sites with Like buttons and who are not Facebook users. The report hypothesizes ways in which Facebook might create profiles of such people based on records of their access to websites that use the Like button.

We are pleased to be able to inform you that our policies and practices do not support the hypotheses that you have put forward.

Most importantly, we can inform you that we do not create pseudonymous profiles of non-users who visit sites with the Like button, either by IP address or by cookie.

We do not do this and have no plans to do it in the future. Even if we wanted to do it, it would be technically impossible using an IP address because when a non-user or non-logged-in Facebook user in Germany visits a site with the Like button, we record a generic IP address in our impression log file rather than a specific one.

It is also our practice not to gather such data about non-users through cookies, including the datr cookie, which is set only when a person visits www.facebook.com and is used to prevent malicious behavior on the Facebook service. Further information about our use of the datr cookie can be found in a detailed Q&A that is attached as an appendix to this letter.

We believe that by offering the Like button within the framework of policies and practices that we have set out below, there is no reason for website owners in Germany not to use this feature.

facebook

It is a matter of great importance to us that we are able to assure people using all aspects of our service in Schleswig-Holstein that they can continue to do so. We hope that by providing this information in both verbal and written form that we have been able to assure you that we have taken your report seriously and responded appropriately.

We are confident that with this clarification of our actual practices and policies, your Office will conclude that the use of Facebook's Like button and Facebook's Pages does not violate German law. We are extremely eager for the many German websites that have made use of the Facebook platform to benefit their businesses and for other purposes to learn that they may continue to use our platform without risk. We would appreciate any guidance you can offer as to the steps we need to take in order to reach an agreed position on the acceptability of Facebook Pages and Like buttons for use by organizations in Schleswig-Holstein.

Please feel free to contact me if you have any further questions or concerns. We look forward to hearing from you on this important issue.

Yours Truly,

Richard Allan
Director of Policy for Europe, Middle East and Africa
Facebook Ireland Limited
Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland
email: ric@fb.com

cc: Eva-Maria Kirschsieper
Policy Manager Germany

Virginie Rousseau
European Legal Counsel

Colm Long
Director of Operations

facebook

APPENDIX-1

Q&A:

What is the Like button?

- The Like button is a social plugin launched in April 2010 as a way for people to share their interest in content off of Facebook (articles, videos, products, etc.) and provide recommendations to their friends back on Facebook.
- The Like button and other social plugins work through an iframe that is served from Facebook and can be placed on any website. The result is that the viewer is accessing a small piece of Facebook right from that website.
- When people who are logged in to Facebook visit a site that uses the Like button or another social plugin, they can have a more personalized experience by, for example, seeing which of their friends have liked a piece of content or liking it themselves and sharing it back with their friends on Facebook.
- Because the Like button is served by Facebook, no user data is shared with the website unless the user has explicitly logged in to the site with Facebook and given it permission to access his or her data.

Do you use the Like button to track people around the web?

- No, we do not track people using the Like button, nor do we create behavioral profiles of them. Profiles on Facebook are made up of information and content explicitly added by the user him or herself.
- We never sell user data to third parties, including advertisers.
- We delete all impression data from social plugins after 90 days.

What impression data do you receive for non-users in Germany?

When a non-user or non-logged-in user in Germany visits a site with the Like button, we receive certain data about the visit including date, time, URL, and browser type. We also record a generic IP address. This sending of information to an entity providing a widget or plugin on a third-party site is a basic feature of the Internet, and we technically cannot prevent it.

How do you ensure that you do not record IP addresses from Germany?

For each impression of the Like button we use a standard geoIP function to identify the country where the communication originated. If this resolves the address to Germany, then a function converts the individual IP address into a common generic IP address at the time when the log file is written. The actual IP address is therefore only used for the necessary and transitory purpose of enabling the communication to take place.

facebook

APPENDIX-2

What impression data do you receive from users in Germany?

When a logged-in user visits a site with the Like button, we receive all of the same impression data described above. We only record a specific IP address if the logged-in user takes an action (e.g., clicks on the Like button). Users consent to this storage of their data when they agree to the terms of our privacy policy.

Why do you need to keep impression data for 90 days?

There is no clear industry standard in this area, and in fact, some companies that provide similar services keep this type of data for much longer. We decided on 90 days because it is enough time for the data to be useful to us if there is a bug, or if we need to make changes to improve our services.

What is the datr cookie?

The datr cookie is a cookie we set when a person visits facebook.com. The cookie allows us to flag and block malicious activity.

We use the datr cookie to determine which user accounts have logged in via a given machine within a recent time window. This provides one of the best signals that we currently have to detect fake or compromised accounts because malicious people will tend to login using many different accounts in a short window of time. The way this is technically implemented is to associate datr cookies (unique machine id) with an array of user ids that have logged in via the given machine on our server. This data is not used for any purposes besides site integrity. Specifically, it is not used for ad-targeting or Insights. The accuracy of this data would be severely compromised if we either cleared the cookie when the user left www.facebook.com (without logging out) or when a social plugin impression occurred.

Does Facebook use the datr cookie to track people across the web?

No, the datr cookie is not used to track people. It is only set when a person visits facebook.com, not when he or she visits a website with a social plugin. Its sole purpose is to help us prevent malicious activity and keep our users safe.

How does information from the datr cookie contribute to Insights?

It does not. We do not use information from the datr cookie in the Insights tool at all.

Why does the datr cookie take two years to expire?

We have found that this is a reasonable amount of time over which to detect patterns of malicious behavior, like unauthorized login attempts, mass creation of accounts, and other attempts to defraud our service.

APPENDIX-3

What are the other tracking tools referenced in the paper (EagleEye, Cavalry, and Nectar) used for?

These were components we previously used with the Like button but subsequently discontinued using when we made optimizations to the Like button. We use these tools for the facebook.com site. Calvary is used to track page-load times on facebook.com. Eagle eye is used to efficiently track user clicks, and Nectar is the generic impression-logging framework that we occasionally need to do via JavaScript in cases where we try to optimize a page load by not sending a request to the server (and instead serving it out of a local cache).