

Submission by „Facebook Ireland Ltd“ to the Office of the Irish Data Protection Commissioner

Response to Complaint(s) Number: 19 & 20

The following submission by “Facebook Ireland Ltd” is a response to complaints filed by “europe-v-facebook.org” before the Irish Data Protection Commissioner as amended by our “request for a formal decision”. It was received by “europe-v-facebook.org” on September 30th 2013.

The submission starting on page 2 of this PDC does only reflect the view of “Facebook Ireland Ltd” and was not changed or amended. The submissions were likely drafted by Facebook Ireland’s law firm “Mason, Hayes & Curran”. We did not receive any addition documents from “Facebook Ireland Ltd”. All other documents of this procedure can be downloaded on “europe-v-facebook.org”.

After we took a first look at the submissions by “Facebook Ireland Ltd” we want to mention the following points, to ensure that any reader will get the full picture of the procedure:

1. In the submissions Facebook Ireland Ltd does in many cases **not responded to our complaints**, but produced arguments and submissions that are irrelevant to the complaints filed. It seems that Facebook Ireland Ltd is trying to “bypass” the arguments we entertained.
 2. In the submissions Facebook Ireland Ltd does in many cases **summarize our complaints** in a way that does not reflect the content of our complaints. We do not know why Facebook Ireland Ltd has chosen this approach other then again “bypassing” the core of the complaints.
 3. In the submission Facebook Ireland Ltd does not respond to the **legal arguments** that were submitted by us, but only focus on facts. The law is not cited in any of the submissions.
 4. In the past 2 years Facebook Ireland Ltd has changed many functions. In the submissions Facebook Ireland Ltd does in many cases **mix the factual situation** throughout this time period. Our complains are usually separating facts and consequences before and after such changes.
 5. In the submission Facebook Ireland Ltd does in many cases refer to the “**audit reports**”. The basis for these reports is not public or independently verifiable. In many cases the DPC has only relied on unverified arguments by Facebook Ireland Ltd when making its assessment. Facebook Ireland Ltd is now relying on these findings, as if they were independently verifiable facts.
- **Therefore we recommend to consult our original complains, as amended by the “request for a formal decision” [\[DOWNLOAD\]](#) when analyzing the submissions from “Facebook Ireland Ltd”.**


COMPLAINTS 19 AND 20 – ‘PICTURE PRIVACY SETTINGS’ & ‘DELETED PICTURES’


1. INTRODUCTION


1.1 Data Use Policy

FB-I’s Data Use Policy clearly informs users of the privacy controls available to them when they post content, including photos, to Facebook:

Whenever you post content (like a status update, photo, or check-in), you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

 *Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.*

 *Choose this icon if you want to share with your Facebook **Friends***

 *Choose this icon if you want to **Customize** your audience. You can also use this to hide your story from specific people.*

1.2 Help Center

FB-I’s [Help Center](#) provides an intuitive and easy-to-use guide to how photos are used on the Facebook platform, and how users can control what happens to their photos when they are uploaded to Facebook. In the “Photos Privacy” section, users are shown all of the privacy features of photos that are uploaded to Facebook. To give one example of many, the Help Center provides the following guidance:

How do I quickly view my photos, and photos I’m tagged in, that are shared with Public?

Your activity log lets you review your photos, and photos you’re tagged in, that are shared with Public. To view photos shared with Public:

- 1. Go to your Activity Log*
- 2. Click **Photos** in the left-hand column*
- 3. Select **Public** from the filter at the top of your **Activity Log** next to **Share with***

*You can also review photos that you’ve hidden on your timeline by selecting **Hidden** from the dropdown menu next to **On timeline**. Keep in mind, photos you’ve hidden on your timeline are still visible to the audience they’re shared with other places on Facebook, such as in Newsfeed and search.*

Each of the remaining options available to users in the Help Center provides focussed step-by-step guidance in relation to the privacy of photos on Facebook.

2. FACTUAL ASSERTIONS MADE BY COMPLAINANT

In the Original Complaints, the Complainant expressed dissatisfaction with the manner in which privacy settings for users’ photos operated on the Facebook platform. These complaints are repeated *verbatim* in the Request for Formal Decision of August 2013. In particular, the Complainant objected to the following features of the photo function on the Facebook platform:

- a) That FB-I had outsourced the delivery of its content, including content relating to pictures posted on Facebook by Facebook users, to an entity known as Akamai.*

- b) *That pictures posted on Facebook were accessible at the URL associated with Akamai despite Facebook privacy settings which ought to have prevented such access. All that was required to view the photo was access to the URL.*
- c) *The Complainant contends that Facebook does not actually maintain a proper access management system for pictures but merely 'hides' links from users and does not block users from the content itself.*
- d) *Users who have accessed any picture can find a link thereto in the cache of a web browser and access the link directly.*

FB-I disputes the accuracy of the Complainant's characterisation of the privacy settings of pictures posted on the Facebook platform and of the security of content distributed by Akamai on behalf of FB-I. In particular, FB-I denies that the Complainant has pointed to a realistic threat to the security of user data.

3. AUDIT PROCESS

3.1 Introduction

The DPC spent considerable time during the Audit Process examining FB-I's security infrastructure in respect of photos posted by users on the Facebook platform. In addressing data security¹ more generally on the Facebook platform, the DPC stated as follows in its 2011 Audit Report:

A dedicated security team therefore worked through security related matters with FB-I throughout the on-site element of the audit and afterwards. Facebook provided its most senior engineering personnel in this area to our Office and made such individuals available on an ongoing basis following the on-site element as more detailed assessments carried out on discrete items as outlined in the Technical Analysis Report.²

During the audit process, the DPC addressed two main issues in connection with photos which are uploaded to the Facebook platform.

First, the DPC considered the security and privacy of photos uploaded to the Facebook platform.

Second, the DPC investigated the process of deleting photos from Facebook and the length of time it takes for photos to be fully expunged from the Facebook platform.

3.2 Security and Privacy of Photos

During the audit, the DPC considered the security and privacy of photos uploaded to Facebook. This was carried out in conjunction with FB-I's most senior security personnel and with the considerable benefit of the analysis contained in the 2011 Technical Audit Report. The DPC was further assisted by Mr Dave O'Reilly of the UCD Centre for Cybersecurity & Cybercrime Investigation. Mr O'Reilly, as an authorised officer of the DPC, was afforded all the rights of access to data held by FB-I as the other members of the DPC audit team.

3.2.1 2011 Audit Report

In appraising the security options available to users to protect the privacy of pictures posted on the Facebook platform, the 2011 Audit Report stated:

Facebook has provided a number of tools to users to enhance their security while they use the site at a desktop or via a mobile device. These tools, which are available to users via Account Settings – Security are assessed in the

¹ The issue of data security generally on Facebook is comprehensively addressed in the Response to Complaint 12 – 'Data Security'.

² Page 107 of the 2011 Audit Report

Technical Analysis Report. We would consider that they do provide a more than reasonable framework for the user who wishes to have in place additional security protection while using the site.³

The 2011 Technical Audit Report noted FB-I's practice of caching static content with the Akamai caching service and described the purpose of using the Akamai service in the following manner:

Akamai maintain a globally distributed network of cache servers that will store copies of content on servers geographically closer to the users of that content than the source servers.

In this particular case, Facebook's data centres are located in the United States and users in locations far from the source servers benefit in terms of user experience when the static content is loaded from Akamai servers that are geographically closer to them⁴

At page 186 of the 2011 Technical Audit Report, the technical expert set out the analysis of the unique photo file names produced by Facebook whenever a user uploads a photo to the Facebook platform. He observed that those file names were comprised of five separate numerical components, that is the volume i.d., the Facebook object i.d., the user i.d., the photo i.d., and a pseudo-random number between zero and 2³¹- 2.

The 2011 Technical Audit Report also noted that the new technique employed by FB-I for generating the random number sequence component of the photo file names was cryptographically stronger than the previous technique employed by FB-I.⁵

At page 188 of the 2011 Technical Audit Report, the following conclusion is drawn on foot of the testing and review carried out on FB-I's systems:

Based on the above analysis, it appears that both the older and the newer techniques generate pseudo-random numbers of sufficient strength that it is not possible to guess the random component of an arbitrary file name.

The simplest way to have possession of the volume ID, Facebook object ID and user ID corresponding to a particular image is to have viewed the image in a browser. In this case, the whole file name is known so the random number will be available and a brute force attack is not required.

...

In conclusion it is believed that, until it is positively demonstrated to be flawed, the process used by Facebook to create photo file names is sufficiently robust to prevent generation of arbitrary, valid photo file names to which an attacker did not already have access.

In reliance on the technical findings, the DPC stated that it was fully satisfied that the practice adopted by FB-I in respect of the privacy of users' photos gave rise to no cause for concern:

This Office is fully satisfied that the randomness of the url string generated for each image is such that there is no realistic possibility of such access taking place unless, of course, a user with access to the image provides the url string of the particular image to a third party.⁶

The DPC also highlighted the fact that in order to gain access to a photo URL in the first instance, a user may have had legitimate access to that photo in line with the photo owner's privacy settings:

Equally, if a user already has legitimate access to an image and therefore the url string, cutting and pasting that string into a browser and accessing the image outside of Facebook does not give rise to any additional concern.⁷

3.2.2 2012 Audit Report

³ Page 108 of the 2011 Audit Report

⁴ Page 186 of the 2011 Technical Audit Report

⁵ Page 187 to 188 of the 2011 Technical Audit Report

⁶ Page 110 of the 2011 Audit Report

⁷ Page 110 of the 2011 Audit Report

The 2012 Technical Audit Report recorded the results of further testing and analysis of the Facebook infrastructure. It dealt with the issue of photo security and privacy in the following brief manner:

It was not been considered necessary to re-perform this testing and the conclusion from the first audit is deemed to stand.⁸

The DPC therefore concluded that:

The position established on this is outlined at Section 1.6 of the Technical Analysis Report. There is no realistic threat in this area.⁹(emphasis added)

3.2.3 Security and Privacy of Photos – Conclusion

After careful examination of FB-I's security systems concerning photos uploaded to Facebook, the DPC has clearly found that FB-I's systems are robust and that consequently, there is little risk of the security or privacy of users' photos being compromised in the manner alleged by the Complainant. The Complainant has not adduced any further factual evidence which would justify a departure from, or a review of, the DPC's finding in this area.

3.3 Deletion of Pictures

During the audit, the DPC considered the technical procedures followed by FB-I when users delete photos or images from Facebook. In particular, the DPC examined the length of time that FB-I retained back-up copies of photos which had been deleted by users. The DPC concluded that no particular security concerns arose in respect of FB-I's practices in this area.

3.3.1 2011 Audit Report

With regard to the accessibility of photos after they have been deleted by a Facebook user, the DPC found that FB-I removes all reference to a photo's URL after it had been deleted by a user:

The assessment carried out was whether it was possible via Facebook to access an image which a user had deleted. We concluded that once the user has deleted the image, Facebook will not provide the Akamai URL at which the deleted image is cached to anyone viewing the user's profile.¹⁰

The DPC observed that the Akamai cache retains content for a period of time after it has been deleted from the Facebook platform, for an average period of 14 days and for no longer than 30 days. The DPC observed:

As above, in order for a third party to retrieve from the Akamai cache a picture that a user has deleted from their Facebook profile, the attacker must therefore have prior knowledge of the photo URL. In such cases, to retrieve the photo URL from Facebook, the user will most likely have viewed the image from the user's profile in their browser. Therefore, they may also have copies of the image cached locally on their PC and/or transparently cached, for example, by their Internet service provider.¹¹

This finding of the DPC reflects the fundamental character of photo sharing on Facebook: in order to access a photo when it has been deleted, any particular user must have had access to that photo before its deletion in order to retrieve the URL and that access will always have been granted in accordance with the privacy settings of the user who has posted the image or photo in question. As noted by the DPC at page 188 of the 2011 Technical Audit Report in such circumstances the whole file name will be available to the user and a 'brute force' attack would not be necessary.

As noted above, once a deleted image drops out of the Akamai cache it will no longer be available at the relevant URL. Furthermore, the fact that images or content which are uploaded to Facebook.com are not

⁸ Page 40 of the 2012 Technical Audit Report

⁹ Page 40 of the 2012 Audit Report

¹⁰ Page 110 of the 2011 Audit Report

¹¹ Page 110 of the 2011 Audit Report

immediately deleted on the request of any user is expressly stated in the Facebook Statement of Rights and Responsibilities at Clause 2.2, which provides as follows:

When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be accessible by others).

3.3.2 2012 Audit Report

The 2012 Technical Audit Report confirms that after a user deletes an image it will be removed by Akamai within 30 days:

The testing has been re-performed as part of this audit and the results described above [results of the 2011 Audit Report] have been replicated¹².

In the DPC's conclusion on this matter in the 2012 Audit Report, it was found that:

We are also satisfied that there is no realistic threat to a deleted image.¹³

3.3.3 Deletion of Photos – Conclusion

The DPC has found that there is no realistic threat to the security of photos after they have been deleted by FB-I's users. The Complainant has not adduced any further factual evidence which would justify a departure from, or review of, the DPC's findings in this area.

4. APPLICATION TO CURRENT COMPLAINT

The Complainant maintains his objection to the manner in which the photo privacy settings operate on Facebook and asserts at page 145 of his Request for Formal Decision that:

"[t]he reports and the technical analysis did not bring forward any new facts or arguments that were not already known in the initial complaints."

The Complainant relies on the following analogy in support of his contention that the security of users' photos uploaded to the Facebook platform is somehow inadequate:

FB-I's security concept works like a hotel room that is opened via a code. The code is not changed when new guests arrive, allowing former guests to get into their former rooms. This problem was not touched.

The analogy relied on by the Complainant is imprecise and likely to mislead the reader for the following reasons:

- i. In order to view any image or photo posted by another user on Facebook, a user must access that photo or image in accordance with the privacy settings of the other user who has uploaded the photo or image in question.
- ii. The complaint ignores the most obvious feature of the photo functionality on the Facebook platform: anytime a particular image is accessible by a Facebook user, it can be copied and saved by that user. There is no need to rely on the URL of that photograph, or the Akamai cache, in order to preserve access to it. As the Complainant's objections presuppose that the photo is accessible by a particular visitor to another user's profile, it is obtuse to object to a much more circuitous and technical means of accessing the photo, where Facebook's standard features would allow straightforward access to the image in accordance with the user's privacy policy with the consequent facility for saving and copying that image provided by most basic devices and terminals used to access the image.

¹² Page 40 of the 2012 Technical Audit Report

¹³ Page 40 of the 2012 Audit Report

In light of the foregoing, FB-I would respond as follows to the Complainant's specific factual assertions:

- a) *That FB-I had outsourced the delivery of its content, including content relating to picture posted on Facebook by Facebook users, to an entity known as Akamai Technologies;*

The caching of photos and images by FB-I on the Akamai platform has been examined by the DPC in the course of the Audit Process and the DPC expressed itself satisfied with the security and legality of this arrangement.

- b) *That pictures posted on Facebook were accessible at the URL associated with Akamai Technologies despite Facebook privacy settings which ought to have prevented such access. All that was required to view the photo was access to the URL;*

Both the 2011 Technical Audit Report and the 2011 Audit Report addressed this issue in detail. The DPC was satisfied that on the basis of the evidence, the random component of a photo's URL was sufficiently robust to minimise the risk of unauthorised access to Facebook users' photos. It was also highlighted that if a user had legitimate access to a photo and chose to copy and paste that photo's URL and open it in a separate browser, no further privacy interest was at risk.

- c) *The Complainant contends that Facebook does not actually maintain a proper access management system for pictures but merely 'hides' links from users and does not block users from the content itself;*

The DPC has comprehensively considered the process whereby links are removed from Facebook when photos are deleted by users and accepted that the underlying file is subsequently deleted from the Akamai cache. No concerns were expressed by the DPC in respect of this process. Users are informed of the possible delay between a user deleting a photo from Facebook and the back-up copies of that photo being deleted at Paragraph 2.2 of the Facebook Statement of Rights and Responsibilities.

- d) *Users who have accessed any picture can find a link thereto in the cache of a web browser and access the link directly;*

The DPC has concluded that there is no risk to a user's photos in the manner described by the Complainant. If a user has access to any picture on Facebook, nothing prevents that user from copying or reproducing that picture without access to the URL itself; in the circumstances, the ability to copy the URL of a photo or to access the photo in the cache of a web-browser presents no further data security risk to Facebook users.¹⁴

¹⁴ Page 110 of the 2011 Audit Report