

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

Response to Complaint(s) Number: 13

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”.**

COMPLAINT 13 – APPLICATIONS

1. BACKGROUND

1.1 What are apps?

Facebook Platform enables users to connect with third-party applications (“apps”), such as Pinterest and Farmville, through Facebook and thereby engage in social activity with their Facebook friends. In order to share their content and activity in apps with Facebook friends, users agree to share information with the apps they and their friends use. Apps receive users’ information via a Facebook application programming interface (“API”) with the user’s permission and in accordance with the Statement of Rights and Responsibilities, which includes special Platform Policies, and the user’s privacy settings. FB-I also provides extensive and helpful information about apps to our users in the Data Use Policy and Help Center.

1.2 Data Use Policy

Facebook provides extensive information about apps, and how they work, in a dedicated section of its Data Use Policy:

About Facebook Platform

Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off of Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.


Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.

Controlling what information you share with applications

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "Applications" or "Apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your [public information](#) and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The “Apps you use” setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.

 *When you first visit an app, Facebook lets the app know your language, your country, and whether you are in an age group, for instance, under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content. If you install the app, it can access, store and update the information you've shared. Apps you've installed can update their records of your basic info, age range, language and country. If you haven't used*

an app in a while, it won't be able to continue to update the additional information you've given them permission to access. Learn more at: <https://www.facebook.com/help/how-apps-work>

💡 Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.

💡 Sites and apps that use Instant Personalization receive your User ID and friend list when you visit them.

💡 You always can remove apps you've installed by using your app settings at: <https://www.facebook.com/settings/?tab=applications>. But remember, apps may still be able to access your information when the people you share with use them. And, if you've removed an application and want them to delete the information you've already shared with them, you should contact the application and ask them to delete it. Visit the application's page on Facebook or their own website to learn more about the app. For example, Apps may have reasons (e.g. legal obligations) to retain some data that you share with them.

Controlling what is shared when the people you share with use applications

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you “like” on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the “Ads, Apps and Websites” settings page. But these controls do not let you limit access to your [public information](#) and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

💡 If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.

1.3 Help Center

Facebook also provides a [detailed FAQ](#) explaining how apps work in its Help Center. This FAQ provides users with practical guidance as to how they can adjust their privacy settings to control the information shared with apps which they and their friends use.

2. FACTUAL ASSERTIONS MADE BY COMPLAINANT

The Complainant objects to the manner in which third-party applications are offered by Facebook Platform. In the Original Complaints, the Complainant appears to make the following main factual allegations, which are reiterated in the 2013 Request for Formal Decision:

- (a) *The providers of applications which are downloaded by a particular user are given access to that user's data without the consent of that user being procured in advance.*

- (b) *Many of the applications hosted by Facebook do not have a privacy policy and that in any event, it would be impossible for FB-I to effectively ensure that application providers have adequate levels of data protection to secure Facebook users' personal data.*
- (c) *Users of Facebook are not aware that if a Facebook friend of theirs installs an application, that application has the ability to access that user's friends' basic profile information such as picture, and name.*
- (d) *While some applications do not require access to the user's friends' personal data, Facebook does not offer a more limited privacy setting in respect of applications than "all the basic information of all friends" to people who wish to avail of the applications function on Facebook.*
- (e) *Users can at all times choose not to use applications or to 'opt-out' of the applications service; the Complainant characterises this choice afforded to users as "all or nothing".*

In the Request for Formal Decision¹, the Complainant further alleges that:

- (f) *FB-I made "no material changes" to its approach to apps following the audit process.*
- (g) *Facebook's app center (which was not in place at the time of the Original Complaints) does not permit users to give "unambiguous consent".*

3. AUDIT PROCESS

3.1 Introduction

Facebook Platform was subject to extensive technical examination during the audit. The DPC also questioned numerous FB-I employees responsible for the day-to-day operation of Facebook Platform.

The DPC's 2011 Audit Report acknowledged the Complainant's concerns in respect of third-party applications, but did not merely confine itself to the Complainant's criticisms when examining the functionality and operation of applications on Facebook. The DPC also had regard to submissions made by the Norwegian Consumer Council which had alleged that some of the terms and conditions imposed on users of applications were complex and unclear. The DPC also addressed certain other matters which arose in the course of the audit itself.

While the DPC's investigations and conclusions with respect to apps were extensive and touched on numerous issues, they can be best understood as addressing three distinct, but related, issues: (a) security; (b) user consent and control; and (c) the use of other users' data.

3.2 Security

FB-I takes the security of user information extremely seriously. Following the audit, the DPC recognised and acknowledged the steps that FB-I takes to prevent apps from gaining unauthorised or improper access to user data.

3.2.1 2011 Audit Report

In the 2011 Audit Report, the DPC specifically considered the steps that FB-I took to keep user data safe:

With the thousands of third-party applications on the Facebook Platform, it is critical that the framework for the provision of data to such applications is as clear and secure as possible. This is recognised by FB-I. It is also the case that while there are matters which are within the direct control of FB-I, others are outside its control as they rest primarily with the third party application. Of course, however it is not possible for FB-I to abrogate responsibility once the information is in the possession of the third party application and it does not seek to do so.

¹ Pages 121 to 125 of the Request for Formal Decision

FB-I highlighted that it endeavours to protect its users from the misuse of their personal data by rouge application and that it devotes considerable resources to doing so.²

The DPC conducted an extensive technical examination of the code underpinning Facebook Platform and questioned the Dublin-based teams with primary responsibility for Facebook apps (the Developer Relations and Platform Operations Teams). The 2011 Audit Report noted that:

[T]he role of Platform Operations is to enforce Facebook's Platform Policy, interacting with developers of third party apps and developers using the social graph, i.e. social plugins to ensure adherence to the platform policy. An examination was carried out of the work queue of the Platform Operations team. It was noted that Facebook has now introduced a number of automated tools, developed in Dublin, to proactively and automatically identify and disable applications engaged in inappropriate activity such as spamming friends or friends of friends, excessive wall postings etc.... The [Platform Operations] Team also responds to specific user complaints regarding the behaviour of applications and enforces a graduated response against the application and the applications provider depending on the nature of the contravention of the Platform policy.³

The 2011 Audit Report further noted that Facebook's real name policy helps to keep users secure, by requiring that a named individual (with a personal Facebook account) be identified as the developer of the app:

It was also pointed out that in line with Facebook's real name culture that all applications (even those developed by the large games developers) must be developed by and attributable to an identifiable user on Facebook.⁴

Following extensive technical testing detailed in the 2011 Technical Audit Report, the DPC confirmed that the security features of Facebook Platform were in line with the position set out by FB-I:

We sought to verify that it is was not possible for an application to access personal data over and above that to which an individual gives their consent or enabled by the relevant settings. The audit verified this is the case.

...

We have confirmed that an application that has been removed by a user can no longer access their information other than that which is publicly available

...

The technical analysis report also confirms that it does not appear possible for an app to perform tasks or access information unless the user has granted an appropriate permission.

...

It is also confirmed that when a friend of a user installing an app has chosen to restrict what such apps can access about them this cannot be over-ridden by the App.⁵

The 2011 Audit Report also suggested two additional steps that FB-I could take to further strengthen security around applications:

First, following extensive technical investigation, the DPC concluded that "authorisation tokens" (in effect, the "key" that allows a user's personal data to be accessed via the API) could, in theory, be shared by developers (though this would breach Facebook's terms and "would lead to the taking of steps against the application by Platform Operations up to and including the taking of legal action against the App Developer"⁶).

This issue does pose a risk to user information in certain limited situations which FB-I acknowledged ... Having considered this matter this Office recommends that FB-I assess this matter in more detail with a view to

² Page 88 of the 2011 Audit Report

³ Page 89 of the 2011 Audit Report

⁴ Page 89 of the 2011 Audit Report

⁵ Pages 92 to 93 of the 2011 Audit Report

⁶ Page 93 of the 2011 Audit Report

*bring forward a solution that addresses these concerns. In the meantime, at a minimum we expect FB-I to advise application developers of their own responsibility to take appropriate steps to ensure the security of authorisation tokens provided by it*⁷

In response to this suggestion, FB-I agreed to provide more messaging to developers highlighting its policy regarding the sharing of authorisation tokens. In addition, FB-I committed to investigate technical solutions to reduce the risk of abuse.⁸

Second, the DPC suggested that FB-I consider introducing further technical safeguards to bolster its reliance on policy and best practice:

*In certain cases reliance is placed on developer adherence to best practice or stated policy to ensure security of user data. This is not considered sufficient by this Office to assure users of the security of their data once they have third party apps enabled. We expect FB-I to take additional steps to prevent applications on a pro-active basis from accessing user information other than where the user has granted an appropriate permission.*⁹

In response, FB-I noted that it has proactive auditing and automated tools designed not just to detect abuse by developers but to prevent it in the first place. FB-I further noted that the findings of the audit would be used to further refine the tools.

3.2.2 Update Report

Following the 2011 Audit Report, FB-I considered the DPC's recommendations to further enhance security around apps. As FB-I noted in the Update Report:

*A primary consideration is safety and security. As detailed in the Report of Audit, FB-I devotes considerable resources to providing a safe and secure Platform. As FB-I previously stated during the audit, FB-I is committed to continuously reevaluating and improving its already impressive safety and security efforts.*¹⁰

FB-I's response to the DPC's security recommendations were set out in the Update Report:

*In its Report of Audit, the DPC confirmed that developers could only access the data that a user gave permission to the developer to access. The DPC expressed concern that developers could share access tokens, the means by which applications get access to Facebook APIs, between applications. For example, a developer could use the application token received for a user adding one of the developer's apps to access that user's data for, presumably, another purpose. The DPC recommended that FB-I explore ways of preventing this from happening, and, at the least, remind developers that sharing of tokens was prohibited. FB-I did in fact explore the possibility and could not determine a feasible solution to this, but did remind developers that sharing of tokens was prohibited in a developer blog post. FB-I does not consider this to be a high risk issue. However, FB-I prevents and/or disables thousands of apps on a daily basis for violations of our policies, detected through both automated and manual means.*¹¹

FB-I also noted that it had introduced additional notifications to make it easier for users to request that their data be deleted from apps:

7.8 Additional Information for Users

*FB-I has also made a change that makes it easier for users to request that their data be deleted from apps that they no longer want to use by including a link to the app's privacy policy directly in the app removal screen. See screenshot below.*¹²

⁷ Page 93 of the 2011 Audit Report

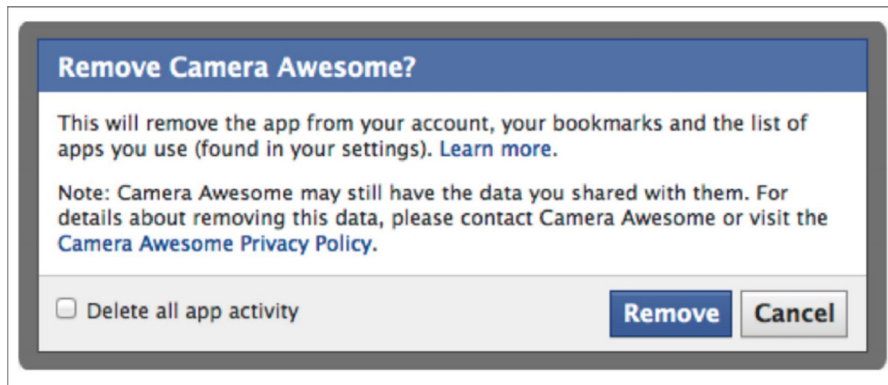
⁸ Page 96 of the 2011 Audit Report

⁹ Page 93 of the 2011 Audit Report

¹⁰ Page 46 of the Update Report

¹¹ Page 47 of the Update Report

¹² Page 61 of the Update Report



3.2.3 2012 Technical Audit Report

FB-I's security safeguards around apps were again examined extensively in the DPC's 2012 audit of FB-I. The results of this technical testing are set out at pages 18 to 25 of the 2012 Technical Audit Report. Key conclusions of this technical analysis include:

It has been re-confirmed that an application that has been removed by a user through their account settings can no longer access the user's basic information

...

It was verified that the HTTP referrer header does not contain the user ID of the browsing user.

...

It has been re-confirmed that only basic information... is accessible when no specific permissions are requested by the application. It has also been re-confirmed that in the same sample cases that were examined in the first audit the permissions behave as documented.¹³

The 2012 Technical Audit Report also considered, in depth, the reasons why FB-I had chosen a bearer token model over a cryptographic signature for granting access to user data via its APIs.¹⁴ Following a consideration of these arguments, the 2012 Technical Audit Report concluded that *"the bearer token model adopted by FB-I provides a reasonable balance between security and usability in the wide range of potential use cases"*.¹⁵

The 2012 Technical Audit Report also revisited those areas where, in the eyes of the DPC, FB-I was overly reliant on developer adherence to policy and best practices. The 2012 Technical Audit Report noted that FB-I had implemented a number of additional technical security measures to improve security here. In particular:

1. Facebook now required that application developers provide a *"secure canvas URL for all new applications created"*¹⁶ (this is a refinement of the previous position where there was no technical safeguard in place to ensure that a secure url was used).
2. The *"offline_access"* token has a validity of 60 days. This reduces the risk in cases where authentication tokens are stolen from a developer.

3.2.4 2012 Audit Report

The 2012 Audit Report noted the security improvements that FB-I had made with respect to apps, and treated the issue as having been satisfactorily resolved.

Addressing the issues with respect to the potential transfer of tokens, the DPC that:

¹³ Page 19 of the 2012 Technical Audit Report

¹⁴ Page 22 of the 2012 Technical Audit Report

¹⁵ Page 23 of the 2012 Technical Audit Report

¹⁶ Page 23 of the 2012 Technical Audit Report

This issue is considered in detail at Section 1.4.7 of the Technical Analysis Report. At the time of the December Audit, it was noted that the alternative to the current authorisation token system was to require an App to generate a cryptographic signature, based on the application secret, for each submitted request for user information. At that time, FB-I provided reasoning for the selection of this architecture. This topic was re-visited as part of the Audit Review, and FB-I having explored alternative solutions presented several additional arguments in favour of the bearer token model as detailed in the Technical Analysis Report. It also took the step of requiring application developers to provide a HTTPS canvas URL with which Facebook can interact which enforces the secure transport of application data.

FB-I does not consider this to be a high risk issue; rather, the more meaningful risk in its view is disreputable applications getting access to user data in the first place. Therefore, this is where it states it directs its efforts as this is something FB-I has more control over and is in a position to act upon disabling what it states as thousands of apps on a daily basis. FB-I has also improved security to the extent possible via the use of the https canvas url. It also reminded developers that sharing of tokens was prohibited in a developer blog post. <https://developers.facebook.com/blog/post/2012/02/03/platform-updates--operationdeveloper-love/> On balance, therefore, it has been concluded that the bearer token model adopted by FB-I provides a reasonable balance between security and usability and no further action is required from FB-I at this time.¹⁷

Considering its recommendation that FB-I introduce further safeguards to prevent unauthorized access to apps, the DPC concluded that:

FB-I has introduced more detailed mechanisms for users to report concerns including privacy concerns in relation to installed apps. Additionally as outlined at Section 1.4.6 of the Technical Analysis Report, FB-I is introducing a new "offline-access" token which will ensure that an installed application that is not accessed by a user will have no ability to access that user's data after a period of 60 days from their last access.

As detailed at Section 7.8 of its Update Report, FB-I has also introduced an enhanced means for users who are removing applications to ensure that any data associated with that application is deleted.¹⁸

3.2.5 Security: Conclusion

Facebook takes user security around apps very seriously and has deployed appropriate technical and administrative safeguards to limit the extent to which apps may gain unauthorized or inappropriate access to user data. These safeguards have twice been subject to extensive technical examination by the DPC. The DPC has also provided advice and guidance to FB-I as to how it can best protect user data in connection with apps. As is noted in the 2012 Audit Report, this advice was adopted by FB-I to further enhance its security processes. In the same report, the DPC indicated that FB-I's security systems around apps, as presently deployed, are in order.

3.3 User Consent and Control

FB-I provides users with extensive information about apps in its Data Use Policy, as set out in Section 1.2 above. In addition, FB-I's approach to capturing user consent for the use of apps was subject to extensive examination by the DPC during the audit process.

3.3.1 2011 Audit Report

During the 2011 audit the DPC extensively considered the information which FB-I provides to users before adding an app. Following this analysis, the DPC found that FB-I could "*significantly improve the manner in which it empowers users via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications*"¹⁹. Consequently, the DPC made four recommendations designed to ensure that users had a full understanding of how their personal data will be used by an app:

First, the DPC recommended that:

¹⁷ Page 31 of the 2012 Audit Report

¹⁸ Page 32 of the 2012 Audit Report

¹⁹ Page 90 of the 2011 Audit Report

*The complexity for a user to fully understand in a meaningful way what it means to grant permission to an application to access their information must be addressed. Users must be significantly empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications.*²⁰

Second, the DPC recommended that:

*It must be made easier for users to understand that their activation and use of an app will be visible to their friends as a default setting.*²¹

Third, the DPC recommended that:

*The Privacy policy link to the third party app should be given more prominence within the application permissions screen and users should be advised to read it before they add an app. This should be supplemented with a means for a member to report a concern in this regard via the permissions screen.*²²

Fourth, the DPC recommended that:

*As the link to the privacy policy of the app development is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live.*²³

3.3.2 Update Report

Between the date of the first audit and the Update Report, FB-I significantly enhanced its approach to apps including through the launch of its app center in early June 2012. FB-I's Update Report provided a detailed overview of the app center and explained how it incorporated the recommendations made by the DPC in the 2011 Audit Report. For ease of reference, the relevant sections are set out in full below:

7.2 User Experience²⁴

There are a number of components to a positive user experience with applications. First, it should be easy for users to find applications on Facebook. Second, Facebook users should be able to tell, generally at least, what an application is about. Third, the user should know what data the application will access through Facebook. Fourth, the user should be presented with the opportunity to read the application's privacy policy. And fifth, the user should have a mechanism on Facebook to report any issues with the application both to the developer and to FB-I. FB-I has made enhancements in all of these areas over the last six months. FB-I's general philosophy is to create an open Platform to allow as many developers to build on—from the smallest to the largest. However, FB-I encourages developers to build quality apps, and FB-I helps drive user traffic to those apps. Demonstrating its commitment to offer users the best app experience, Facebook launched an App Center in early June 2012.

Facebook's App Center is a centralized location for users to find high-quality apps on Facebook and, importantly, to learn in one place about the way in which those apps use data obtained from Facebook. It is accessible from the user's homepage, but also, it is featured during the new user experience. The advantage to featuring it when during the new user experience is that users are taken to the high quality apps on Facebook, all of which must meet certain requirements to be listed in App Center, and users are presented with extensive information about the apps. See screenshots below:

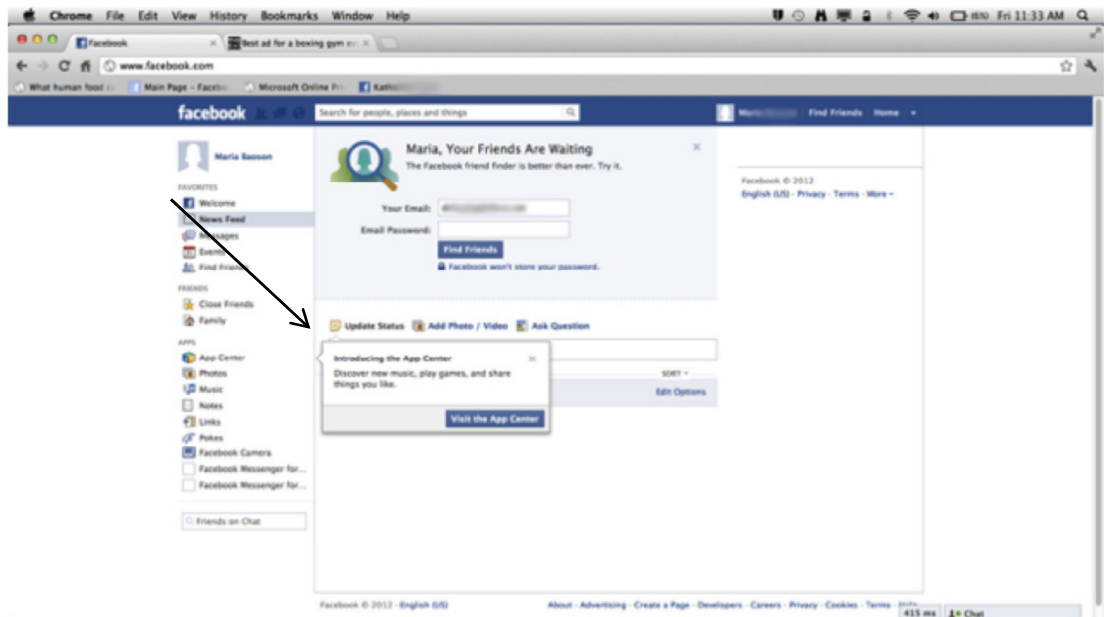
²⁰ Page 94 of the 2011 Audit Report

²¹ Page 94 of the 2011 Audit Report

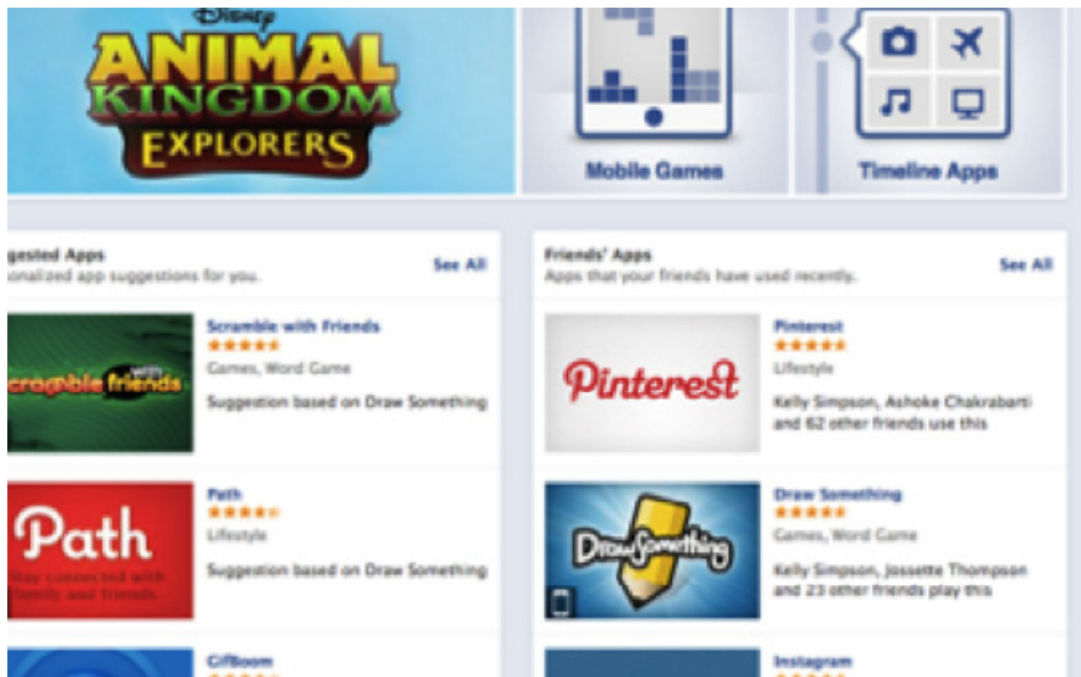
²² Page 94 of the 2011 Audit Report

²³ Page 95 of the 2011 Audit Report

²⁴ Pages 47 to 56 of the Update Report

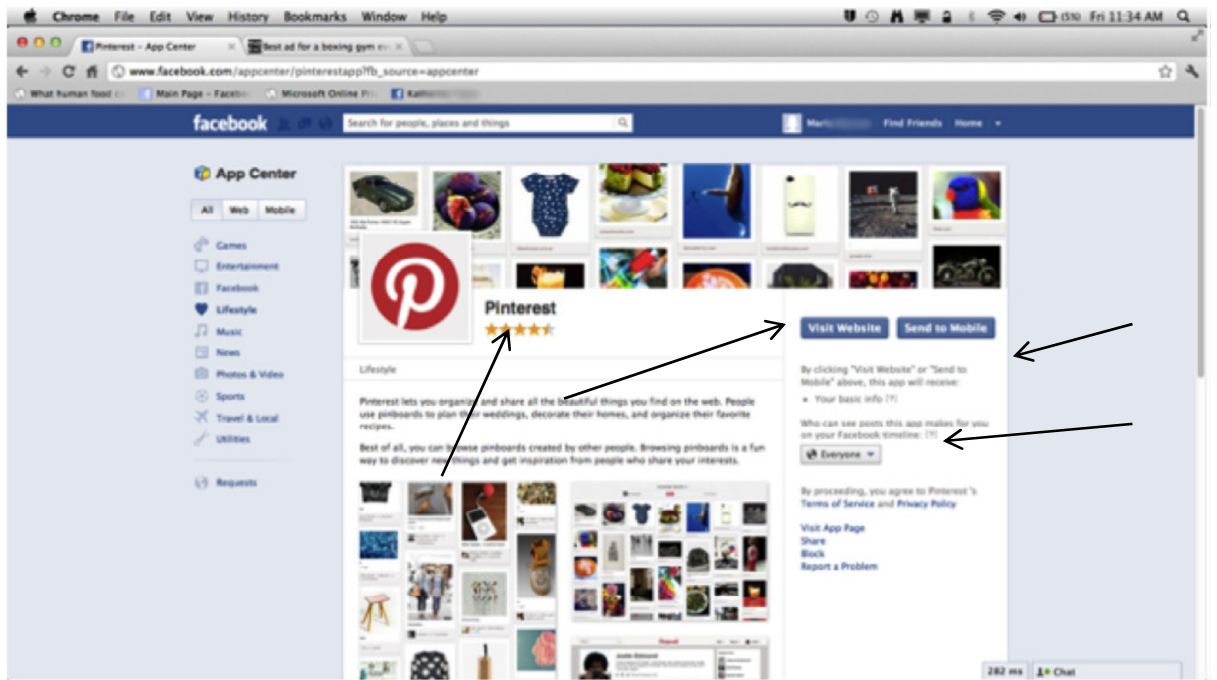


(part of the new user experience)



(landing page for the app center)

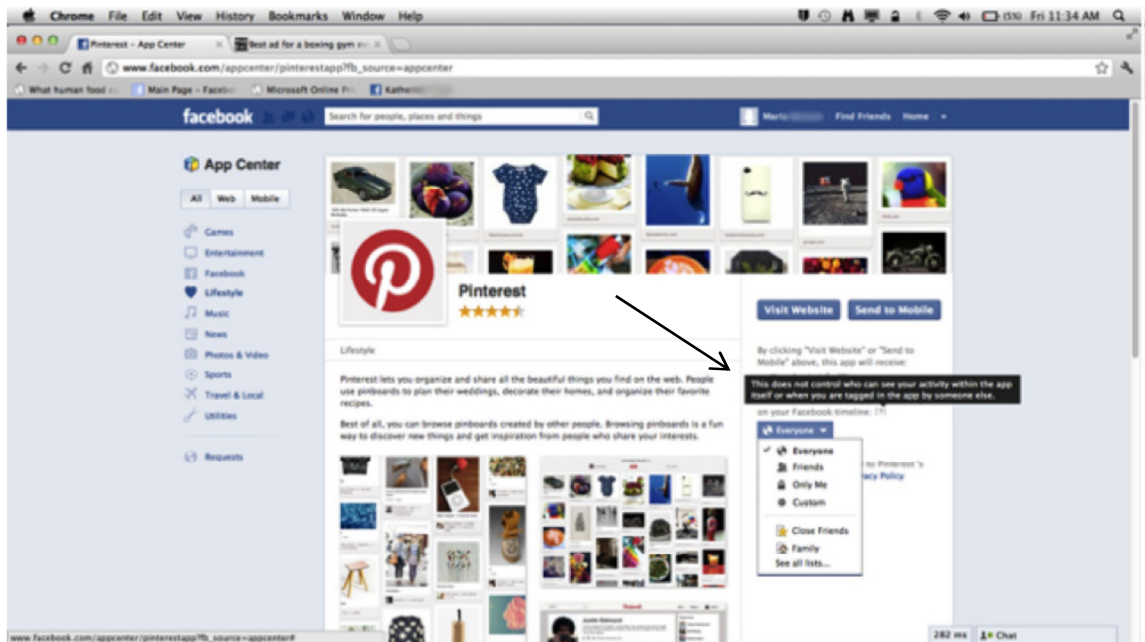
From the app's landing page when a user clicks on the app in the center, the user can: 1) learn about the app; 2) visit the app's website; 3) read the app's privacy policy and terms of use; 4) set the audience for posts the app makes to Facebook Timeline on the user's behalf; 5) see the categories of data the app will get if the user adds the app; 6) see the app's rating; 7) block the app; 8) visit the app's page; 9) report a problem; and 10) see the app's publisher.



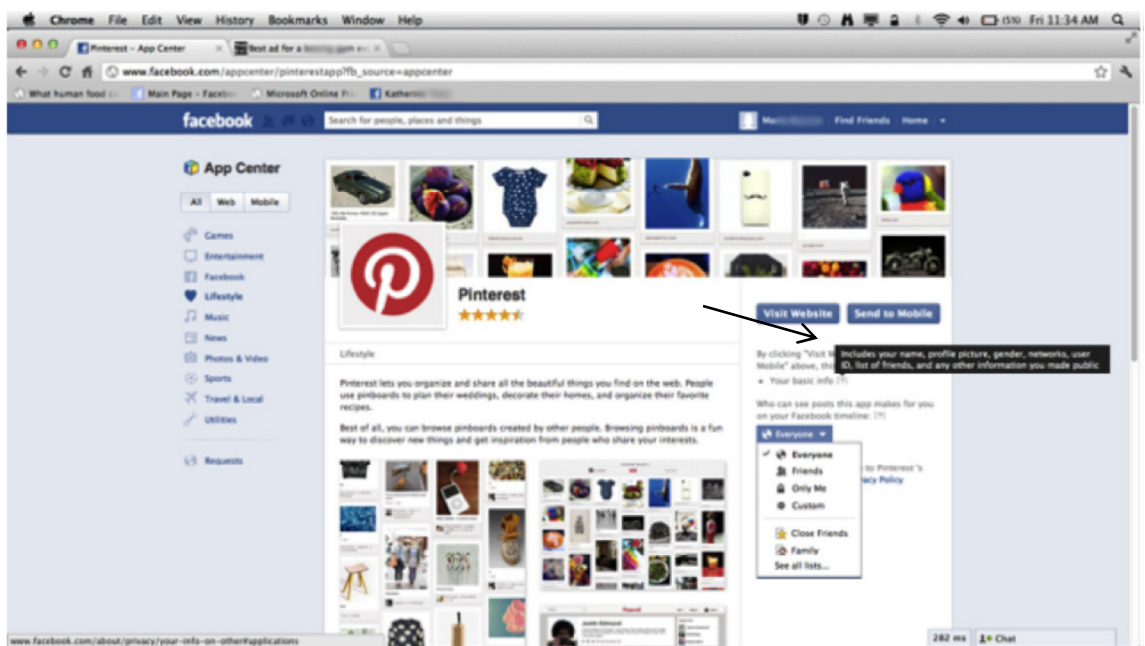
(landing page for app when user clicks on it from app center)



(audience control before adding app)



(information when user clicks on "(?)" associated with audience selector)



(information when user clicks on "(?)" associated with "basic info")

Report or Contact SongPop

Report to Facebook

- I'm reporting the app for spam
- I'm reporting this app as inappropriate
- I'm reporting how this app is using my information
- I'm having an issue with a payment or virtual goods purchase in SongPop

Contact the developer

- I'm reporting a bug or a loading issue within the app
- I'm reporting abusive content within the app
- I want to send my own message to the developer

Screenshot (optional). [How do I submit a screenshot?](#)

No file chosen

[Hide Uploader](#)

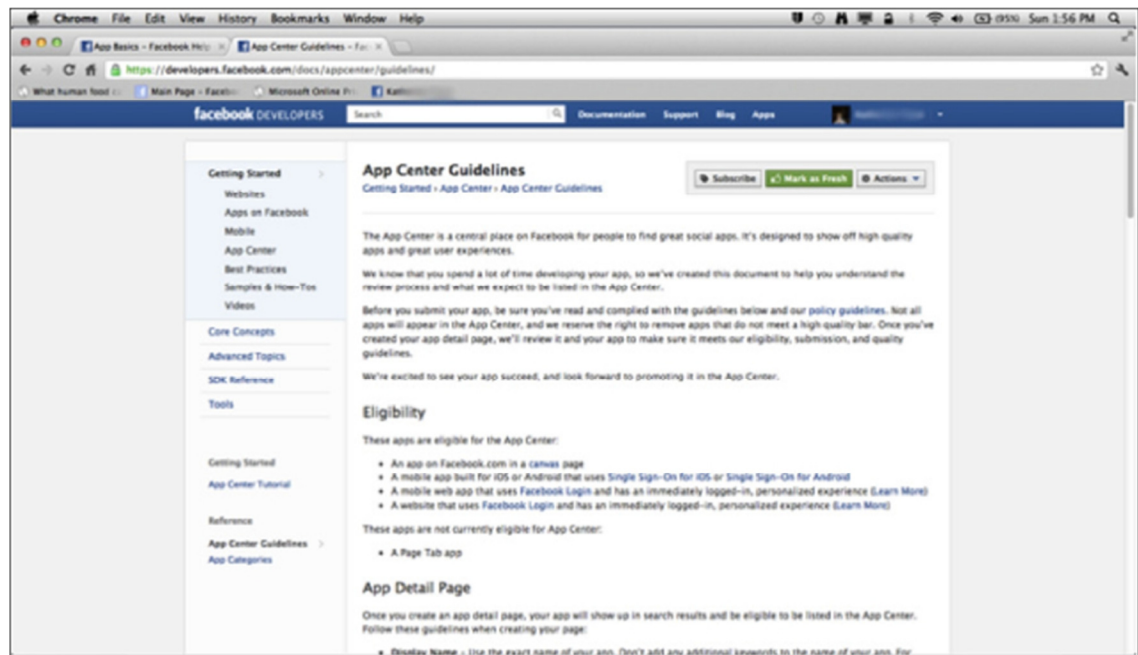
Is this your intellectual property?

(report form)

(privacy policy and terms of service of app)

In order to be listed in the App Center, an app must agree to follow special guidelines. See guidelines here: <https://developers.facebook.com/docs/appcenter/guidelines/>.

See screenshot below:



To encourage the building and maintaining of quality apps, Facebook offers developers an app rating metric in Insights to report how users are rating the app. Furthermore, Facebook uses a variety of signals, including user ratings and engagement, to determine whether an app is eligible to be listed in or should be removed from the App Center.

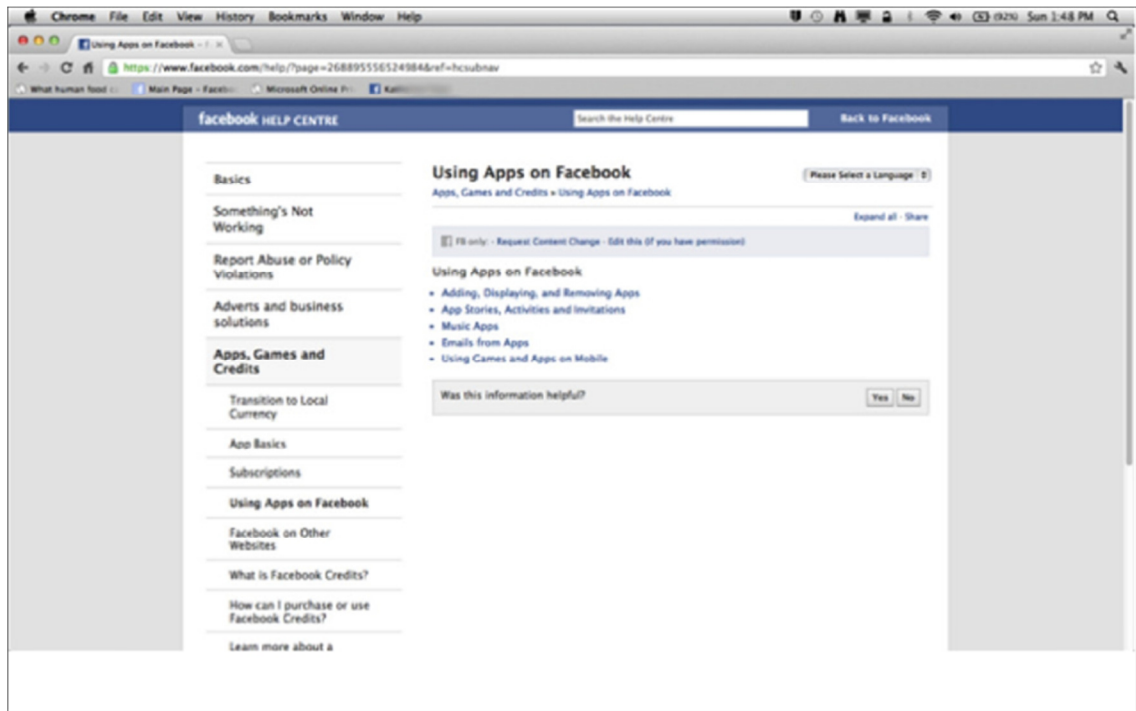
Another part of the user experience of apps on Facebook is the accessibility of information about how to find and use app privacy settings. FB-I provides easy to find information in its Help Center about where users can control their settings. See <https://www.facebook.com/help/218345114850283>

See screenshot below:



FB-I also provides easy to find information about using apps in general in its Help Center. See <https://www.facebook.com/help/?page=26889556524984&ref=hcsubnav>.

See screenshot below:



Finally, as described in section 2.3 (new user education), FB-I has added resources to the new user experience on using apps.

7.3 Tools for Monitoring Developer Compliance

In the Report of Audit, the DPC expressed concern that 1) users were not told by FB-I to read the app's privacy policy, and 2) an app's privacy policy might have a broken link. FB-I believes that by requiring developers to have a privacy policy that is provided to users before and after they add an app, FB-I is providing users with the ability to exercise choice as to whether to read the policy and agree to the use of their personal data by the app. The privacy policies in App Center apps are presented in the right-hand column where users look to see what data the app will need and where they can choose the visibility setting for their app activity. Privacy policies are similarly included in all permission dialog boxes for apps that are not part of the App Center.

FB-I also developed and implemented a technology to check for the presence of a privacy policy in the permissions dialog box in apps on canvas and to ensure that the link to the policy is active. FB-I has a policy for warning developers with missing or dead links and for disabling the app if the developer does not correct the problem. Since the tool was built, FB-I has been testing it to work through any bugs and expects it to be fully operational in the beginning of October.

....

7.5 Reporting Apps

In the Report of Audit, the DPC recommended that there be a means within the permission dialog box for users to report an app. Although FB-I's permission dialog box already contained a "report app" link, FB-I's Platform Operations team has worked during the past six months on various reporting flows to provide users with more efficient and intuitive options, including to contact the developer to express a concern or to report the application to FB-I directly.

Some examples include introducing the ability to report an app for how it uses data. See screenshots below.

Report or Contact Horoscopes

Report to Facebook

- I'm reporting the app for spam
- I'm reporting this app as inappropriate
- I'm reporting how this app is using my information

Choose a type of issue ▾

- The developer has not deleted my information as requested
- The app is asking for information it does not need

Co

- I'm reporting abusive content within the app
- I want to send my own message to the developer

Screenshot (optional). [How do I submit a screenshot?](#)

no file selected

[Hide Uploader](#)

Is this your intellectual property?

Report or Contact Horoscopes

Your report has been sent to Facebook. If you no longer wish to interact with this app, you can remove or restrict it.

Is this your intellectual property?

FB-I tracks the number of reports any given app receives for reporting reason and if the report number reaches a certain threshold, FB-I investigates.

FB-I has also provided a direct means for a user to contact the developer of an app. See screenshots below.

Report or Contact Horoscopes

Report to Facebook

- I'm reporting the app for spam
- I'm reporting this app as inappropriate
- I'm reporting how this app is using my information

Contact the developer

- I'm reporting a bug or a loading issue within the app
- I'm reporting abusive content within the app
- I want to send my own message to the developer

Would you like to send a message to the app developer? If so, this entire report will be sent to the app developer. We will only pass on the information you provide in the report to the app developer, in addition to your user ID. This is needed to help the app developer address your issue.

To: Horoscopes

Your Email:

Optional. Only provide one if you want the app developer to be able to respond if needed.

Additional Details (required):

Screenshot (optional). [How do I submit a screenshot?](#)

no file selected

[Hide Uploader](#)

Is this your intellectual property?

Report or Contact Horoscopes

Your report has been sent to Facebook. If you no longer wish to interact with this app, you can [remove](#) or [restrict](#) it.

Is this your intellectual property?

There are report link for apps on Canvas ([facebook.com](https://www.facebook.com)), in GDP (permissions dialogue box), and in App Center.

3.3.3 2012 Audit Report

The DPC's 2012 Audit Report noted, favourably, the enhancements that FB-I had made to its app registration flow. Considering each of its recommendations in turn, the DPC first noticed the steps that FB-I had taken to ensure that users are "*sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications*".²⁵

In its 2012 Audit Report, the DPC stated:

*FB-I has introduced improvements in this area which are detailed in Chapter 7 of its Update Report. Before installing an application, there is now clearer information provided beside where the "install app" button is located detailing what user information the application will use prior to installation. There is also an on-screen means available for a user to make an informed choice as to the audience for any posts which the app might make on their behalf, as well as the audience for who will see that the user has added the app.*²⁶

FB-I's innovative and streamlined new app center was also favourably referred to by the DPC, which stated that the development would tend to streamline and standardise the user experience in interacting with apps on Facebook. The DPC felt that these developments by FB-I "*have provided a means for users to exercise choice based on clear information prior to taking a decision to install an app*"²⁷.

Turning to consider the DPC's second recommendation that "*it should be made easier for users to understand that their activation and use of an app will be visible to their friends as a default setting*"²⁸, the DPC considered the new audience selector tool and was satisfied that it was now clear to a user of apps who, if anyone, would see that the user has added the app as well as who would see any activity which the app might post to the user's timeline.

Considering his third recommendation that the "*privacy policy link to third party app should be given more prominence*"²⁹, the DPC noted that the application permissions' screen had been redesigned so as to display the privacy policy link and the ability to report and block an application. While the DPC noted its preference that users be explicitly encouraged to read the app's privacy policy, it was accepted that the "*app's privacy policy is suitably placed to encourage such an action by a user who wishes to do so*".³⁰

Turning to the fourth and final recommendation that FB-I engineer a tool which would detect any privacy policy links for applications which are broken or no longer operational, the DPC noted that he was satisfied that:

*FB-I adopted this recommendation and brought forward an internal tool which ensured that all applications available from the site had an active privacy policy link. This tool was first used in July and, according to FB-I, has been intermittently operational now for a number of weeks as FB-I works through bugs.*³¹

3.3.4 Consent and Information: Conclusion

Between the date of the first and second audits, FB-I significantly enhanced the way it empowers its users to make informed decisions with respect to apps. These changes took on board all of the relevant recommendations made by the DPC during the first audit, and were positively received in the second audit report. In addition, it is important to recall that FB-I's disclosures in the app center are supported by the extensive and helpful information provided to users in the Statement of Rights and Responsibilities, the Data Use Policy and Help Center.

In summary, FB-I's approach to giving users control over apps has been developed in consultation with the DPC and, following extensive technical examination and questioning of relevant personnel, was approved by the DPC in the 2012 Audit Report.

²⁵ Page 29 of the 2012 Audit Report

²⁶ Page 29 of the 2012 Audit Report

²⁷ Page 30 of the 2012 Audit Report

²⁸ Page 30 of the 2012 Audit Report

²⁹ Page 30 of the 2012 Audit Report

³⁰ Page 30 of the 2012 Audit Report

³¹ Page 30 of the 2012 Audit Report

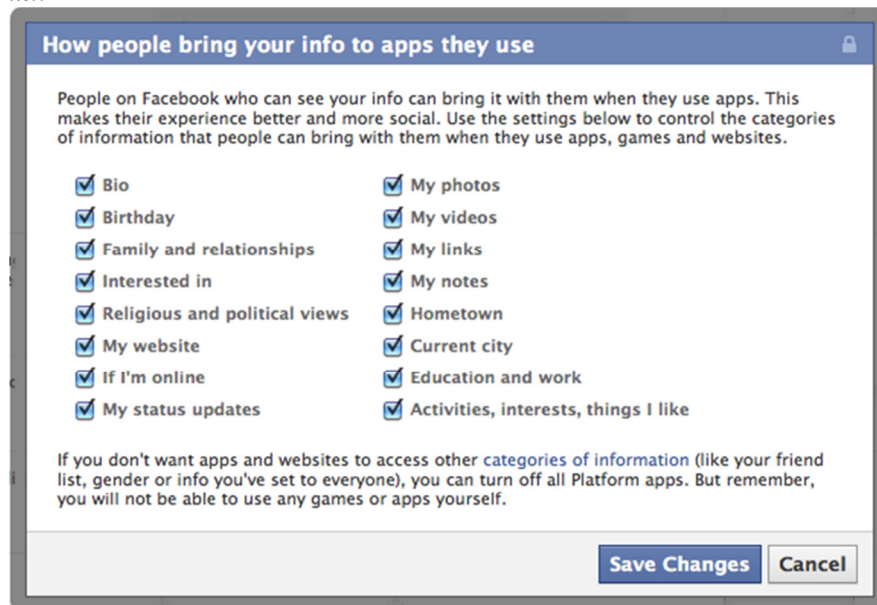
3.4 Use of other Users' Data

Third-party apps on Facebook are designed to allow for *social* engagement. As noted in the Data Use Policy:

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list - which includes your User ID - so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the [Ads, Apps and Websites](#) settings page. But these controls do not let you limit access to your [public information](#) and friend list.



If you want to completely block applications from getting your information when your friends and others use them, you will need to [turn off all Platform applications](#). This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.

3.4.1 2011 Audit Report

The DPC considered, in depth, this *social* aspect of apps on Facebook during the audit. Section 5.5 of the 2011 Technical Audit Report explained how the social aspect of apps works:

Access to User Friend Information

When a user authorises an application, that application can request access to the same information about that user's friends as the user has access to. This access is not granted by default and must be specifically requested by the application. For example:

- User A starts using an application.
- User A authorises the application to access their friend's photos.
- User B is a friend of user A.
- User B has some photos that are only shared with friends.
- User B has not indicated via privacy settings that their photos should not be shared with applications that their friends use.

The application will have access to User B's photos.

Unless the friend has opted out as described below, the same basic information listed in Section 5.2³² is also available to the application about each of the user's friends.

Users can control what information the applications that their friends are using can see about them. This configuration is carried out in Privacy Settings->Apps and Websites in the section titled "How people bring your info to apps they use". The user can unselect any of the aspects of their profile that they do not want shared (except basic information). It has been confirmed that if, in the above example, User B has unchecked "My Photos" in this privacy configuration, an application installed by User A can no longer see User B's photos. This is true even if User A has authorised the application to view their friend's photos.

Note that User A will still be able to interactively view User B's photos by browsing to User B's profile, but applications installed by User A will not.

If a user does not want any information shared with applications that their friends install, including basic information, they must disable the application platform. This is achieved by selecting "Turn off all platform apps" in Privacy Settings->Apps and Websites. It has been confirmed that if the user decides to do this, applications that their friends install will have no visibility of them, including basic information. However, when the application platform is disabled the user will not be able to use any applications themselves.³³

On foot of this technical analysis, the DPC noted that:

When a user grants access to their information they can also grant access to information related to their friends. The extent to which the application can access information relating to friends is determined by the settings of the friend. When a friend of a user adds an application, the default setting (where the user has not proactively changed their privacy settings) allows the third party application joined by a friend to access your profile picture and name.³⁴

The DPC further concluded that:

We verified that when a friend of a user installing an app has chosen to restrict what such apps can access about them that this cannot be over-ridden by the app.³⁵

While the DPC was satisfied with the privacy controls offered by FB-I, it recommended that the relevant options be moved from the "privacy settings" area of the site to the "apps section"³⁶. Consequently, the DPC concluded its consideration of this issue by noting that "*it should be made easier for users to make informed choices about what apps installed by friends can access personal data about them.*"³⁷

FB-I agreed to "*positively examine alternative placements for the app privacy controls so that users have more control over these settings*".³⁸

³² The basic information listed at Section 5.2 of the Report is User ID, Name, Profile Picture, Gender, Age Range, Locale, Networks, List of friends, any other information the user has made public.

³³ Pages 167 to 168 of the 2011 Technical Audit Report

³⁴ Page 90 of the 2011 Audit Report

³⁵ Page 95 of the 2011 Audit Report

³⁶ Page 20 of the 2011 Audit Report

³⁷ Page 95 of the 2011 Audit Report

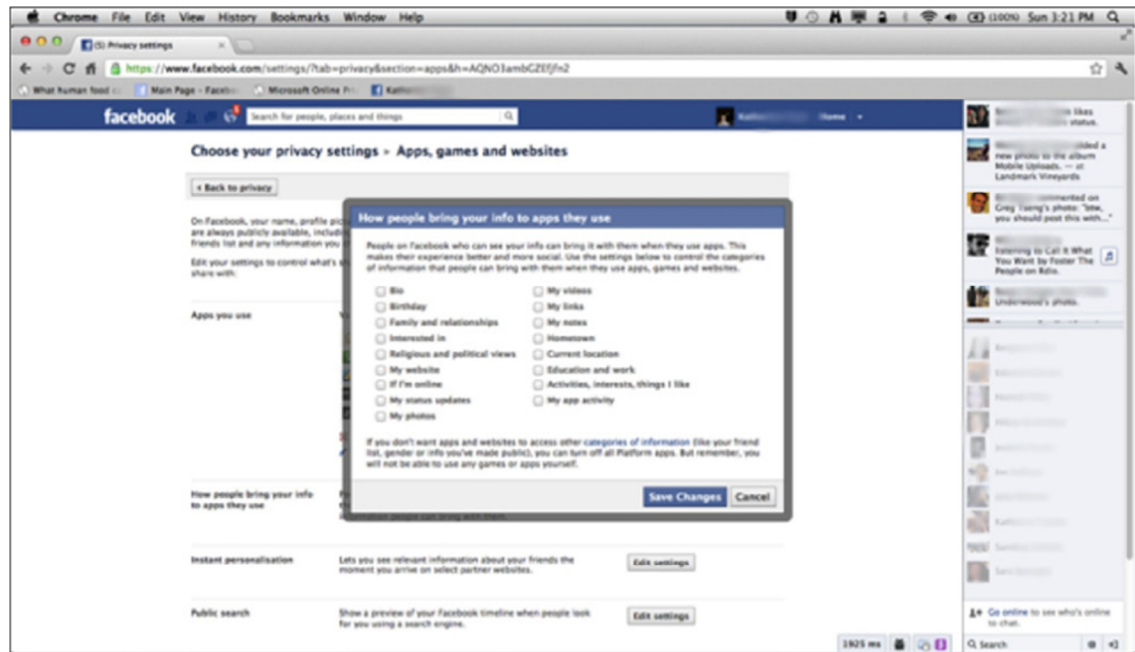
³⁸ Page 95 of the 2011 Audit Report

3.4.2 Update Report

Section 7.4 of the Update Report noted that Facebook had implemented a number of the DPC's suggested improvements to give users greater control over how their data is used.

7.4 Permission for App to Access Friends' Data

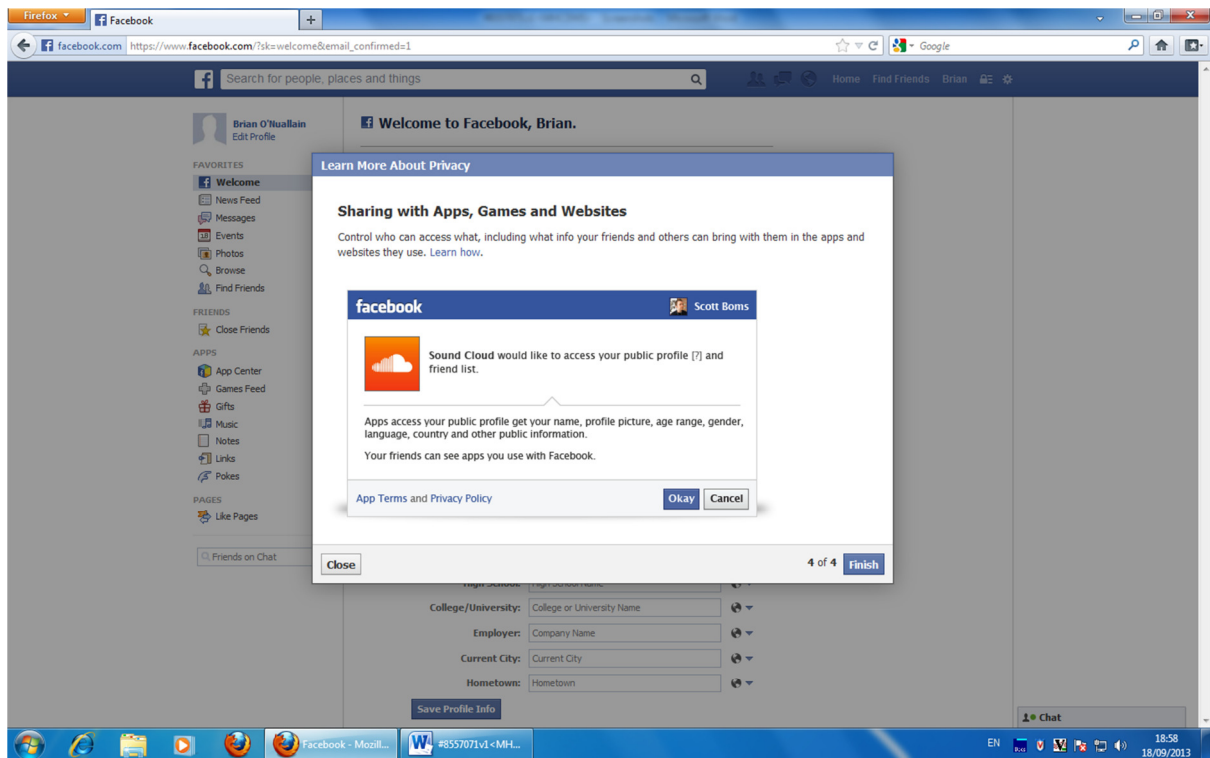
FB-I has made some enhancements to its education of users about how apps can obtain, with the user's permission, some data of the user's friends. First, the setting that allows users to control the private data that an app can access if one of their friends adds the app and gives it permission is located with the other app settings in the privacy settings. See screenshot below:



Second, to offer information about this setting to the new user, FB-I has added resources to the new user experience explaining how to use apps and the app settings.³⁹

Further details of the information about apps provided to new users are set out in Section 2.6 of the Update Report where it is noted that when a new user takes the “privacy tour” they are provided with information about the core parts of Facebook, including sharing with apps. See screenshot of current functionality below:

³⁹ Page 54 of the Update Report



3.4.3 2012 Audit Report

In the 2012 Audit Report, the DPC again verified, on foot of technical testing, that a user could control the extent to which their friends shared their personal data (See Section 1.4.5 of the 2012 Technical Audit Report).

The 2012 Audit Report also suggested that FB-I consider the extent to which FB-I could “*examine introducing a means for a user who did not wish for anything other than their basic data to be available to apps installed by their friends without having to actually take the rather drastic step of turning off apps altogether*”.⁴⁰

FB-I further considered this issue following the audit. As is noted above, FB-I allows its users to exercise granular consent over the extent to which a user’s friends can transfer their data to apps. Such control is exercised via two tools.

First, a user is provided with a straightforward option to toggle Platform on or off. If a user turns Platform off, none of their data will be shared with apps.

Second, users who wish to exercise more precise and granular control over the data their friends can share with apps, while still participating in apps themselves, may use their privacy settings to control which of their information can be provided to apps. Facebook currently allows users to choose whether to let their friends share the following categories of data with apps:

- Bio
- Birthday
- Family and Relationships
- Interested In
- Religious and political views
- My website
- If I’m online

⁴⁰ Page 31 of the 2012 Audit Report

- My status updates
- My photos
- My videos
- My links
- My notes
- Hometown
- Current City
- Education and Work
- Activities, interest and things I like
- My App activity.

This degree of granular control allows users to choose how they wish to let their friends share their personal data with apps. The DPC broadly accepted the appropriateness of this level of control when noting, in its 2012 Annual Report, that all outstanding matters in the audit had been progressed to its satisfaction.

4. APPLICATION TO CURRENT COMPLAINT

In light of the position as set out above, FB-I would respond to the Complainant's material factual allegations as follows:

- (a) *The providers of applications which are downloaded by a particular user are given access to that user's data without the consent of that user being procured in advance.*

This is incorrect. Users add apps via a flow which has been reviewed and approved of by the DPC and which provides the user with detailed information on the way in which data will be shared.

FB-I does share a limited amount of non-personal information with an app when a user first visits an app. This is disclosed in the Data Use Policy which provides that:

When you first visit an app, Facebook lets the app know your language, your country, and whether you are in an age group, for instance, under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content.

- (b) *Many of the applications hosted by Facebook do not have a privacy policy and that in any event, it would be impossible for Facebook Ireland to effectively ensure that application providers have adequate levels of data protection to secure Facebook users' personal data.*

Following consultation with the DPC, FB-I deployed technical tools that check for live links to privacy policies of apps on Platform. These efforts were reviewed, and approved of, by the DPC during the audit process. Most importantly, Facebook's Platform Policies require that apps have privacy policies and otherwise comply with all applicable laws.

- (c) *Users of Facebook are not aware that if a Facebook friend of theirs installs an application, that application has the ability to access that user's friends' basic profile information such as picture, and name.*

This is incorrect. FB-I's Data Use Policy expressly describes this. FB-I also gives users granular control over the extent to which their friends may be able to share their personal data with applications.

- (d) *While some applications do not require access to the user's friends' personal data, Facebook does not offer a more limited privacy setting in respect of applications than "all the basic information of all friends" to people who wish to avail of the applications function on Facebook.*

As noted above, FB-I gives users granular control over the extent to which their friends may be able to share their personal data with applications. Furthermore, users may turn off Platform completely, in which case none of their data will be shared by their friends with apps their friends use.

(e) Users can at all times choose not to use applications or to 'opt-out' of the applications service; the Complainant characterises this choice afforded to users as "all or nothing".

This is not an all or nothing choice. Alongside the straightforward ability to turn on and off apps, users are also given an ability to choose whether or not their friends can share certain categories of data (such as their birthday, or their interests) with apps.

In the Request for Formal Decision, the Complainant further alleges that:

(f) That FB-I made "no material changes" to its approach to Apps following the Audit.

This claim is baseless. Not only did Facebook significantly enhance its approach to apps in light of the DPC's recommendations, but also refined its approach to apps when Facebook launched app center.

(g) That Facebook's App Center (which was not in place at the time of the original complaints) does not permit users to give "unambiguous consent".

This position is unsustainable and groundless. As is noted above, the app center provides users with clear information about apps, the permissions they seek, and the extent to which the use of that app will be visible to other users on the site. The app center was considered extensively by the DPC during the 2012 audit and was favourably received.