An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Facebook Ireland Ltd

Report of Re-Audit

21 September 2012

Table of Contents

Chapter 1 Executive Summary

In December 2011, this Office published the results of a detailed audit of Facebook Ireland (FB-I). The audit contained a list of detailed, time-lined "best practice" recommendations addressed to FB-I. It provided for a review of implementation of these recommendations, with a formal review in July 2012. This Report summarises the outcome of this review.

The review consisted of a detailed, point-by-point, examination of FB-I's implementation of our recommendations. In practice, it was a rolling review, involving ongoing detailed consultation with FB-I as the indicative deadline for each recommendation approached. We also asked our Technical Consultant, Dave O'Reilly, to verify the implementation of a sample of the recommendations. His report is included at Annex 1.

The preparation of the report also involved ongoing consultation with other data protection authorities (DPA) - notably in the context of the EU's Article 29 Working Party and its Technology Sub-Group – so as to ensure that their particular concerns were accommodated to the maximum extent possible. The fact that our recommendations were couched in terms of "best practice" rather than mere legal compliance facilitated such accommodation of other views.

As with the main audit, FB-I cooperated with the review process, while vigorously defending its point of view, particularly where our recommendations, or the views of other DPAs, challenged the general philosophy of the company. This was true, for example, in relation to the company's insistence on maintaining its requirement that users use their real names on the network.

The company's formal response to our recommendations – included at Annex 2 to this Report – demonstrates the constructive approach adopted by the company.

Our Report summarises the degree of implementation of our "best practice" recommendations as of the date of publication (21 September 2012). It shows that most of the recommendations have been fully implemented to our full satisfaction. This is particularly in the areas of better transparency for the user, better user control over settings, clear retention periods for the deletion of personal data or an enhanced ability for the user to delete items, the user's right to have ready access to their personal data and the capacity of FB-I to ensure rigorous assessment of compliance with Irish and EU data protection requirements. In some cases – notably in relation to the "tag suggest" feature – FB-I has in fact gone beyond our initial recommendations, at our request, in order to accommodate the views of other DPAs.

In a small number of cases – notably new user education, deletion of social plug-in impression data for EU users, fully verified account deletion beyond all doubt and minimising the potential for ad targeting based on words and terms that could be considered to be sensitive personal data - full implementation has not yet been achieved but is planned to be achieved by a specified deadline. It is also clear that ongoing engagement with the company

will be necessary as it continues to bring forward new innovations. The value of such engagement to identify and deal with any data protection concerns prior to launch is fully accepted by FB-I. Such discussion is also necessary in relation to new issues that arose in the course of the review – for example, the balance to be struck between FB-I's duty to protect young users from sexual predators, through monitoring certain user behaviour and reporting reasonable suspicions to relevant authorities, and the need to ensure that such monitoring and reporting is proportionate to the danger of serious consequences for young victims.

It is clear that this Review is no more than an assessment at a point in time of FB-I's compliance with its data protection obligations to its users. As indicated above new developments in terms of services to users and use of their data for advertising purposes will continue to throw up challenges to FB-I's strengthened in-house compliance function. It will also involve continued detailed involvement of our Office's oversight role, including responding to issues raised by other DPAs and by the many data subjects for whom FB-I is the data controller.

As with the earlier Audit Report, this review Report does not involve formal decisions by the Office on the complaints it has received in relation to FB-I. The audit has taken account of the substantive issues raised in these complaints and it can be expected that at least some of these issues will have been dealt with to the satisfaction of the complainants. However, any complainant has the right to require the Commissioner to make a decision on her/his complaint(s) where an "amicable resolution" of the complaint can not be achieved and to appeal that decision to the Courts if it is not to their satisfaction. We will now move to addressing any outstanding complaints, in accordance with our normal procedures.

I would like to thank Dave O'Reilly for his professionalism in understanding our requirements and meeting them within often unrealistic deadlines. I would also like to thank our team in the Office and our intern Claire Murphy from the Horizon Doctoral Training Centre at the University of Nottingham who spent three months with us during the course of the review and whose understanding and research on emerging issues proved to be a valuable input to the process.

Gary Davis
Deputy Commissioner
21 September 2012

List of Recommendations and Findings – Status

Privacy Policy / Data Use Policy

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Privacy & Data Use Policy Complexity & accessibility of user controls	FB-I must work towards: • simpler explanations of its privacy policies • easier accessibility and prominence of these policies during registration and subsequently • an enhanced ability for users to make their own informed choices based on the available information	Satisfactory response from FB-I with more precise details regarding education efforts with existing users to be provided to this Office within four weeks
	The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page.	Satisfactory response from FB-I

Advertising

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Advertising Use of user data	There are limits to the extent to which user-generated personal data can be used for targeted advertising. Facebook must be transparent with users as to how they are targeted by advertisers	Satisfactory response from FB-I
	FB-I does not use data collected via social plug-ins for the purpose of targeted advertising	Unchanged
	FB-I should move the option to exercise control over social ads to the privacy settings from account settings to improve their accessibility. It should also improve user knowledge of the ability to block or control ads that they do not wish to see again	Satisfactory response from FB-I
	If, FB-I in future, considers providing individuals' profile pictures and names to third parties for advertising purposes, users would have to provide their consent.	n/a
	The current policy of retaining ad-click data indefinitely is unacceptable.	Satisfactory response from FB-I
	There is a requirement for a change in policy and practice in relation to the possibility of targeted advertising utilising Sensitive Data[1]	Four week period for FB-I to address concerns outlined by this Office
	The availability and use of features on site that allow users to filter and block certain types of ads does not appear well known to users and FB-I is therefore asked	Satisfactory response from FB-I

[1] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

	to take steps to better educate users about the options which they present to control ad content[2]	

Access Requests

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	TARGET IMPLEMENTATION DATE	STATUS
Access Requests	If identifiable personal data is held in relation to a user or non-user, it must be provided in response to an access request within 40 days, in the absence of a statutory exemption	In line with the schedule in relation to availability from the user's profile, their activity log and the download tool. Data will be added to the various tools in phases, beginning in January 2012.	Satisfactory response from FB-I with the exception of uploaded photo metadata which will be available from the end of October.

Retention

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Retention of data	The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved.	Satisfactory response from FB-I
	User's should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis.	Satisfactory response from FB-I with the exception of an acceptable period for the deletion of images with FB-I requested to provide details of an amended procedure within 4 weeks of this date
	Users must be provided with a means to exercise more control over their addition to Groups	Satisfactory response from FB-I
	Personal data collected must be deleted when the purpose for which it was collected has ceased	Satisfactory response in general from FB-I but subject to a further review from this Office in relation to social plug-in impression data subject that was subject to a litigation hold
	There is not currently sufficient information in the Data Use Policy to educate users that login activity from different browsers across different machines and devices is recorded.	Satisfactory response from FB-I
	We have confirmed that data entered on an incomplete registration is deleted after 30 days	Process changed so this issue no longer arises
	Data held in relation to inactive or de-activated accounts must be subject to a retention policy	We are satisfied with the information provided by FB-I on the justification for the current approach to retention. FB-I to revert within 4 weeks in relation to an appropriate means to contact account holders who have deactivated

[2] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

		their accounts or are inactive. Application of exceptions to 6 month deletion period for disabled accounts to be examined

Cookies / Social Plug-Ins

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Cookies/Social Plug-Ins	We are satisfied that no use is made of data collected via the loading of Facebook social plug-ins on websites for profiling purposes of either users or non-users.	Re-confirmed
	It is not appropriate for Facebook to hold data collected from social plug-ins other than for a very short period and for very limited purposes	Dealt with in Retention Section
	FB-I to supply more detailed information to this Office within four week's of today's date on the use of the fr cookie and the consent collected for this cookie	Ongoing with FB-I to revert in Four weeks

Third Party Apps

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Third Party Apps	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 sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications	Satisfactory response from FB-I
	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	Satisfactory response from FB-I
	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.	Satisfactory response from FB-I
	As the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live.	Due to bug issues not operational at present and therefore will be re-examined when operational
	We verified that it 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.	Re-confirmed
	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. However, it should be made easier for users to make informed choices about what apps installed by friends can access	FB-I should re-examine providing choice to their users short of turning off the ability to use Apps altogether

	personal data about them. The easiest way at present to manage this is to turn off all apps via a user's privacy settings but this also prevents the user from using apps themselves.	
	We have identified that the authorisation token granted to an application could be transferred between applications to potentially allow a second application to access information which the user had not granted by way of the token granted to the first application. While this is a limited risk we recommend that FB-I bring forward a solution that addresses the concerns outlined. 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 the authorisation tokens provided by it.	Satisfactory response from FB-I
	We do not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. We do note however the proactive monitoring and action against apps which breach platform policies. However, 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 from accessing user information other than where the user has granted an appropriate permission.	Satisfactory response from FB-I

Disclosures to Third Parties

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Disclosures to Third Parties	The current Single Point of Contact arrangements with law enforcement authorities when making requests for user data should be further strengthened by a requirement for all such requests to be signed-off or validated by a designated officer of a senior rank and for this to be recordable in the request. We also recommend that the standard form used require all requesting entities to fully complete the section as to why the requested user data is sought so as to ensure that FB-I when responding can form a good faith belief that such provision of data is necessary as required by its privacy policy. FB-I should also re-examine its privacy policy to ensure that the current information provided is consistent with its actual approach in this area.	Satisfactory response from FB-I

Facial Recognition / Tag Suggest

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	STATUS
Facial Recognition/Tag Suggest	FB-I should have handled the implementation of this feature in a more appropriate manner and	FB-I will provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts	Implemented. FB-I has also agreed to delete collected templates for EU users by 15 October and to agree a process for collecting consent with this

	we recommended that it take additional steps from a best practice perspective to ensure the consent collected from users for this feature can be relied upon	with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings. FB-I will discuss with this Office any plans to extend tag suggest to allow suggestions beyond confirmed Friends in advance of doing so.	Office if it chooses to provide the feature to EU users again.
	We have confirmed that the function used to delete the user's facial profile is invoked when the user disables "tag suggestions".		Re-confirmed

Data Security

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Security	Many policies and procedures that are in operation are not formally documented. This should be remedied.	Satisfactory response from FB-I
	We are satisfied that FB-I does have in place an appropriate framework to ensure that all access to user data is on a need to know basis. However, we recommended that FB-I expand its monitoring to ensure that there can be no employee abuse through inappropriate password resets of a user's account	Satisfactory response from FB-I
	We were concerned that the tools in place for ensuring that staff were authorised to only access user data on a strictly necessary basis were not as role specific as we would have wished.	Satisfactory response from FB-I
	We are satisfied that there is no realistic security threat to a user photo from their upload to Akamai. We are also satisfied that there is no realistic threat to a deleted image	Position as stated in December Audit
	We believe that current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data via "screen scraping" while allowing the service to be effectively provided to legitimate users.	Position as stated in December Audit

Deletion of Accounts

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	OUTCOME
Deletion of Accounts	There must be a robust process in place to irrevocably delete user accounts and data upon request within 40 days of receipt of the request (not applicable to back-up data within this period.)	Given the scale of the task, a satisfactory response from FB-I pending resolution or clarification

		within four weeks on image deletion and log de-identification, with group content to be deleted in early 2013

Friend Finder

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Friend Finder	We are satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder purposes.	Reconfirmed
	We recommend that users be made aware that where they choose to synch their contact information from a mobile device, those contact details are transmitted in plain text and are therefore not secure during transmission. This is not an issue within Facebook's control but users should nevertheless be made aware when choosing this option.	Data now securely transmitted
	We established that the action of disabling synchronisation does not appear to delete any of the synchronised data. This requires an additional step via the "remove data" button within the app. We recommend that it should be clear to users that disabling synching is not sufficient to remove any previously synched data.	The released version of the iPhone App has addressed this issue. FB-I to revert to this within 4 weeks on the addition of disclosure to the Android version of the app.
	We were concerned that the facility whereby businesses could upload up to 5,000 contact email addresses for Page contact purposes created a possibility of the sending of unsolicited email invites by those businesses in contravention of the *e*Privacy law with an associated potential liability for FB-I. We recommended a number of steps to be taken to address this risk	Satisfactorily addressed by publication of December Audit and re-confirmed
	We confirmed that passwords provided by users for the upload of contact lists for friend-finding purposes are held securely and destroyed	Re-confirmed

Tagging

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Tagging	There does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it.	Taking account of the various tools available to users to manage Tags and to delete them if they so wish we are not requiring an ability to prevent Tagging at this time.

Posting on Other Profiles

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Posting on	We recommend that FB-I introduce increased functionality to	We are satisfied with the

Other Profiles	allow a poster to be informed prior to posting how broad an audience will be able to view their post and that they be notified should the settings on that profile be subsequently changed to make a post that was initially restricted available to a broader audience. We recommend the sending of a notification to the poster of any such change with an ability to immediately delete their post if they are unhappy.	information provided by FB-I on the operation of this function

Facebook Credits

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Facebook Credits	We are satisfied that FB-I does act as a data controller in the provision of the Facebook Credits service However, we would consider that it is not fully apparent to users using the service that FB-I is acting as a data controller and that information generated in the context of their use of Facebook Credits is linked to their account. It is recommended that the Data Use Policy be significantly expanded to make clear the actual personal data use taking place in the context of Facebook Credits.	Satisfactory response from FB-I pending further clarification emerging from the operation of FB-PI

Pseudonymous Profiles

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION
Pseudonymous Profiles	We consider that FB-I has advanced sufficient justification for child protection and other reasons for their policy of refusing pseudonymous access to its services

Abuse Reporting

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION
Abuse Reporting	We are satisfied that FB-I has appropriate and accessible means in place for users and non-users to report abuse on the site. We are also satisfied from our examination of the User Operations area that FB-I is committed to ensuring it meets its obligations in this respect.

Compliance Management / Governance

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Compliance Management/ Governance	We found that the compliance requirements for the conduct of direct marketing by electronic communications means had not been fully understood by certain FB-I staff members engaged in marketing. We recommend that documented procedures be developed to ensure that data protection considerations are taken fully into account when direct marketing is undertaken either by or on behalf of FB-I and that appropriate training be given to staff and contractors.	Complete at the time of publication of the December Audit
	This Office requires that Irish data protection law and by extension European data protection laws be fully addressed when FB-I rolls-out a new product to its users. We recommend therefore that FB-I take additional measures in the first half of 2012 to put in place a more comprehensive	Ongoing. All significant changes to the use of personal data with a data protection impact to be approved by FB-I in a manner

	mechanism, resourced as appropriate, for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law.	set out by the Board of FB-I that takes full account of European data protection requirements.

Chapter 2
Subject Matter Areas Examined During the Audit

A continuous assessment of FB-I's compliance with the recommendations made during the initial audit took place throughout 2012. Daily emails, phone calls and videoconferences were utilised to ensure that FB-I was clear on the changes to be made to comply with the recommendations. The on-site element of the re-audit once again took place over six days, 2-3 May and 10-13 July 2012.

Full cooperation was again received from FB-I during the re-audit.

In the following sections, FB-I's response to the recommendations made in the Audit report is assessed. FB-I has largely implemented the recommendations as detailed in the text. Of course there will always be issues of detail and interpretation in this area with new issues continuing to arise so by its very nature any such assessment can only be considered to be an assessment at a specific point in time.

2.1 Privacy Policy / Data Use Policy

Recommendation: Simpler explanations of its privacy policies
FB-I has implemented a revised data use policy which was brought forward following intensive consultation and negotiation with this Office. In a complex online environment such as that in which FB-I provides services, a privacy policy/data use policy is considered by this Office to serve only as a useful baseline for how personal data is used by a data controller. Reliance on a privacy policy alone as a legal basis for processing personal data may not on its own meet the requirements for consent outlined in the Data Protection Acts 1988 & 2003. We also recognise that approaches to what should be contained in a privacy policy are developing and clearly therefore this is an area in which we expect FB-I and all other data controllers established in Ireland to be closely monitoring and iterating their policies to reflect best practice. Conversely, such continuous refinement must also take account of the fact that constantly updating such policies can be annoying for users and potentially confusing. Data controllers need to take account of such considerations before revising privacy policies.

Recommendation: easier accessibility and prominence of these policies during registration and subsequently

Recommendation: The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page

Recommendation: an enhanced ability for users to make their own informed choices based on the available information

FB-I has amended the user registration process considerably in close consultation with this Office. Firstly it has re-engineered the initial user registration screens so as to ensure that no

user personal data is collected before an opportunity arises for a new user to read the terms of service, data use and cookies polices. The prominence of this information was increased and it was placed before the "Sign Up" button. Additionally in a small but significant step FB-I agreed to remove the phrase "and understand" in the agreement language. It was the view of this Office that due to the nature of social networking, a new user may benefit from some hands-on experience before they will fully understand the implications of a privacy policy.

FB-I has also amended the subsequent registration screens by including for the first time contextual information which informs users what specific use will be made of uploaded contacts, their profile photo and their education and employment information. For the first time users are also allowed to amend the visibility of the education and employment information on the registration screen itself. While the initial default setting on screen is set to public for adult users, as a non-public setting does not allow Facebook to suggest existing users with those characteristics, it can be changed at a click of a button.

These screens are also now supplemented by a "welcome dashboard" which gives specific prominence to the privacy settings on the site and encourages the user to take a tour which focuses on the areas which this Office considered give rise to potentially the greatest privacy risk and the greatest need for education: the use of timeline, sharing on Facebook, Tagging and Apps.

These screens as the key initial means by which new users engage with Facebook are critical in terms of incubating and developing the notion of privacy and control of privacy in new users. We will therefore continue to keep this process under close review to ensure that new users are empowered to make informed choices in relation to their privacy.

Of course, providing information and choices to users during and immediately upon sign-up when they have not even used the site while useful may not fully serve the aim of educating users. This Office was concerned that users would not engage at that point. Taking these concerns on board, FB-I is implementing a privacy prompt for all new users after they have used the site for 30 days. That period of time is chosen to reflect a reasonable period of time when a user will have developed a working knowledge of the site.

As stated above, reliance upon the Facebook Data Use Policy as the sole means for capturing user consent for the use of their information may not always be considered acceptable by this Office for all possible uses of data. This is the same standard that we apply to all organisations. The means of collecting consent favoured by this Office once a person has joined a particular service is what we term "just in time" or in FB-I's terms "inline". During the course of the audit and indeed before it had begun, FB-I had increasingly moved towards a model of providing "inline" controls to users. This reflects this Office's preference in this area that when a user is making a choice or asked to make a choice about how they wish their personal data to be used that they are presented with relevant understandable information at that time on which to base their choice. This will principally arise in relation to proposed new uses of their personal data.

We have impressed upon FB-I that this is the standard to which they will be held in such circumstances and clearly this will remain an area that will be closely examined by this Office

as Facebook continues to innovate which we accept it must do but must be done in a way that takes full account of data protection requirements.

We had also asked that efforts be directed towards the education of existing users on the site. It is clear that the focus of FB-I was directed principally at new users and that this area did not therefore receive the same attention. FB-I has indicated that "along with new user education, FB-I is committed to providing education, contextual where appropriate, to users about new products and features, including reference to privacy and/or visibility controls associated with the new product or feature, as well as periodically refresh users' knowledge of existing privacy and visibility controls through various means. We therefore expect to receive precise proposals from FB-I in this area within four weeks of today's date.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Privacy & Data Use Policy Complexity & accessibility of user controls	FB-I must work towards: • simpler explanations of its privacy policies • easier accessibility and prominence of these policies during registration and subsequently • an enhanced ability for users to make their own informed choices based on the available information	Satisfactory response from FB-I with more precise details regarding education efforts with existing users to be provided to this Office within four weeks
	The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page.	Satisfactory response from FB-I

2.2 Advertising

In the Audit report, it was indicated as follows "this Office does not consider that it is possible using data protection requirements as a basis to require FB-I to deliver a free service from which members can have the right to opt-out completely from the means of funding it. However, there is an absolute necessity that members be fully aware of what information generated in their use of the service will be used for advertising purposes thereby allowing them to exercise choice. Equally, we consider that Irish data protection law imposes reasonable limits as to what information generated by a member should be considered as usable for advertising purposes under Facebook's form of consent."

It is clear that in the intervening period that Facebook has accelerated the pace of innovation in relation to advertising. Relevant developments are detailed in Chapter 3 of FB-I's Update Report. Any such innovations however must take account of the basic requirements outlined above of transparency informing choice with a limitation of use in certain

circumstances. The focus of our review therefore was to ensure that these requirements were met.

Recommendation: There are limits to the extent to which user-generated personal data can be used for targeted advertising. Facebook must be transparent with users as to how they are targeted by advertisers.
As outlined earlier, the revised Data Use Policy contained a large number of amendments agreed with this Office. In relation to advertising this included revisions to FB-I's description in section IV of *'How Advertising and Sponsored Stories Works'*

The following information was added:

> We use the information we receive to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook. Learn more at: https://www.facebook.com/help/?page=226611954016283

With regard to Keywords from status updates and Search Terms, specifically, FB-I has stated that

> FB-I discloses in its Data Use Policy that it may use any data it receives to target ads. There are some limitations, however, and FB-I understands that certain forms of advertising may call for additional notice and consent. However, when FB-I has done a privacy and legal analysis and found the use of a category of data to be permissible under the consent it receives through its Data Use Policy and the law, FB-I does believe it is acceptable to use the data for ad-targeting purposes. For example, in response to the recommendation of the ODPC that it give users better notice that it may use keywords from status updates to inform its ad-targeting, FB-I included further information about this use of data in its revised Data Use Policy.

FB-I also referred to its practice of bundling characteristics (ad topics) which might include aggregated topics. For example, FB-I indicated that an interest such as "photography" and a reference in a post to "wildlife" might result in an aggregated topic "nature" being created in response to advertiser demand. If an advertiser thus wanted to appeal to a certain cohort of users by selecting "nature" as a keyword, users may be aggregated into a "nature" category again in real time. FB-I has indicated that such "topics" are refreshed typically every two weeks.

This Office is satisfied that the Data Use Policy provides appropriate information to users in relation to the potential use for advertising purposes of keywords from any status updates they make on the site. We have also clarified with FB-I that such use of keywords is undertaken in real time and no such keywords are stored against the user account or profile. Where an individual is attributed with a "topic" in the manner outlined above, such topics as long as they remain attributed to an individual are available in response to an access request in the user's expanded archive. This was a key issue of individual user transparency for this

Office and one which was recognised by FB-I. We have therefore not raised any further concerns in relation to this use of data.

Limitations on Use of Data

Targeted Advertising based on Sensitive Data

Targeted advertising based on sensitive data was also specifically addressed in the 2011 audit report of FB-I with this Office stating that in terms of this practice:

> "Taking into account the reassurances provided in the Advertising Guidelines versus what appears to be possible, we would recommend that, at a minimum, there is a requirement for a change in policy and practice in this area."[3]

FB-I responded with a commitment at that time that

> "FB-I undertakes to clarify its policy in this respect, which is to allow targeting on the basis of keywords entered by the advertiser but not allow targeting based upon the described categories of sensitive data." (p.50)

However, the advertising tool allows an advertiser to select terms from what is effectively an automatically-generated dictionary. FB-I clarified that these terms do not place users into categories, but are rather dynamically created from all the content on the site. So, for instance an advertiser can select "socialist" and reach anyone connected to pages that have the word "socialist" in their name. This could include a wide range of different content types including "I hate socialists" and "I love socialists" pages as the system is simply pulling together content around the particular word. This is similar to the way that a search engine will return all content related to a word automatically.

FB-I in its Update Report stated

> "As the DPC noted in the Report on Audit, FB-I's Advertising Guidelines prohibit targeting based on a user's personal characteristics within sensitive categories. FB-I undertook to clarify its policy in this respect, which is to allow targeting on the basis of keywords entered by the advertiser but not allow targeting based upon the described categories of sensitive data.

FB-I has categorically reiterated that it does not allow targeting based upon the described categories of sensitive data in a person's profile such as religious or political views and the 'basic information' section in the user profile which might indicate a user's sexual orientation. Here, a user can (if they wish) highlight whether they are interested in men or women (both options are presented as radio buttons and both options can be selected).

However, we note that ad targeting excluding described categories of sensitive data is not addressed in FB-I's Data Use Policy and this Office remains of the view that this needs to be clarified in the Data Use Policy or other appropriate place. FB-I in response has pointed to its Advertising Guidelines, https://www.facebook.com/ad_guidelines.php, which according to it

[3] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

expressly prohibit using sensitive data for ad-targeting purposes. This Office however remains concerned that there is a significant gap between a policy prohibiting the use of sensitive data for ad-targeting purposes and effective enforcement given that words and terms which are clearly sensitive in nature can be used by advertisers when targeting ad campaigns. This remains a significant concern to this Office and one on which we consider FB-I should be doing more either to further limit the practice or seek explicit consent from their users as would be required by data protection law. We are therefore giving FB-I a further period of 4 weeks to consider this issue and present solutions to this Office. We are affording FB-I this period as up to this point this matter was not put to it in these terms.

Messages and Chat

While this Office was satisfied following engagement with FB-I and the clarification that emerged in the Data Use Policy that the use of keywords within status updates for advertising purposes would not be considered surprising by users, we remain firmly of the view that it would be a surprise for users if keywords were extracted from the content of messages and chat on the site for advertising purposes.

FB-I has clarified that it does not conduct ad-targeting based on the content of messages and chat on the site. This Office sought to conduct a technical analysis to confirm this was the case by assessing all scans sent to messages[4] on the site. This task while technically feasible was ultimately not undertaken at this point due to time constraints during the process. As it happens, during the course of the audit a concern arose from comment in the media as to scanning of messages that was taking place for what was stated to be the prevention of crime. While this has transpired to be focused solely on the prevention of child sexual grooming, this is nevertheless an area on which this Office will need to work with FB-I to ensure that all such scanning takes place taking full account of data protection requirements. This engagement will provide the context in which a definitive examination of the use of content from messages and chat will take place.

Conclusion: FB-I does not use data collected via social plug-ins for the purpose of targeted advertising

The technical analysis conducted on site again examined the use of data collected via social plug-ins. We remain satisfied that no advertising related queries are served to the impression data collected from social plug-ins on websites.

Recommendation: FB-I should move the option to exercise control over social ads to the privacy settings from account settings to improve their accessibility. It should also improve user knowledge of the ability to block or control ads that they do not wish to see again

Implemented as outlined in consent/data use policy section

Recommendation: The current policy of retaining ad-click data indefinitely is unacceptable.

This matter is addressed in Section 2.3 of the Technical Analysis Report. This recommendation is implemented except in relation to financial data. Additionally from a

[4] Messages in this context solely relates to intra-site communications between users using Facebook servers and equipment. It does not include email communications sent to or from members on the site using electronic communications networks

transparency perspective any actual ads clicked by a user are available to the user via their download tool.

Recommendation: The availability and use of features on site that allow users to filter and block certain types of ads does not appear well known to users and FB-I is therefore asked to take steps to better educate users about the options which they present to control ad content[5]

FB-I added a section on influencing the ads one sees to its About Advertising page, which is accessible by clicking on the sponsored story icon on the ads received.

Ad Targeting below 20 users/Information available to advertisers

There were no specific recommendations made to FB-I in the December Audit on this issue. These issues were examined again on-site during 2012 with the position remaining as outlined in the December audit namely that ads cannot be served to a group of below 20 users and that there are limitations to the information available to advertisers with no personal data disclosed.

Cookies/Third Party Cookies

FB-I as indicated earlier has produced a dedicated cookie notice which was separately highlighted to all users when it captured a new user agreement to its data use policy. In addition, FB-I has placed a link to its cookies policy on the end of all pages on the site which should ensure that any user seeking such infomration can automatically access it. Such an approach may be considered to achieve compliance with the requirements of Statutory Instrument 336 of 2011 which implemented the ePrivacy Directive in Ireland in relation to those first party cookies dropped by FB-I.

The most appropriate manner of implementing the requirements of the ePrivacy Directive, particularly with respect to third party and behavioural advertising cookies remains a matter of discussion at present. This Office, together with others, had hoped that more concrete proposals and action would emerge from the W3C do not track[6] discussions that would have common applicability; although, it now appears that this is unlikely at least in the short to medium term. Our Office, similar to designated enforcement authorities in this area across the EU, is required to ensure that the provisions of the law in this area are implemented. In this context, when a regulatory consensus emerges from enforcement authorities with respect to the manner in which consent should be obtained in a behavioural advertising context, we would expect FB-I to review its practices and procedures in this area to ensure proper compliance.

This Office will be directing its attention to the necessary steps to be taken in relation to the capture of consent for behavioural advertising cookies and will expect FB-I to implement such a mechanism when a consensus emerges between enforcement authorities. FB-I has indicated that it is actively engaged in the W3C discussions and will remain in communication with this Office regarding its compliance in these areas.

[5] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

[6] http://www.w3.org/2011/tracking-protection/

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Advertising Use of user data	There are limits to the extent to which user-generated personal data can be used for targeted advertising. Facebook must be transparent with users as to how they are targeted by advertisers	Satisfactory response from FB-I
	FB-I does not use data collected via social plug-ins for the purpose of targeted advertising	Unchanged
	FB-I should move the option to exercise control over social ads to the privacy settings from account settings to improve their accessibility. It should also improve user knowledge of the ability to block or control ads that they do not wish to see again	Satisfactory response from FB-I
	If, FB-I in future, considers providing individuals' profile pictures and names to third parties for advertising purposes, users would have to provide their consent.	n/a
	The current policy of retaining ad-click data indefinitely is unacceptable.	Satisfactory response from FB-I
	There is a requirement for a change in policy and practice in relation to the possibility of targeted advertising utilising Sensitive Data[7]	Four week period for FB-I to address concerns outlined by this Office
	The availability and use of features on site that allow users to filter and block certain types of ads does not appear well known to users and FB-I is therefore asked to take steps to better educate users about the options which they present to control ad content[8]	Satisfactory response from FB-I

2.3 Access Requests

In our December Audit Report this Office indicated as follows: "The right for an individual to access personal data held by a data controller established in the EU is a basic right enshrined in the Data Protection Acts and the EU Data Protection Directive. The right of access grants a

[7] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

[8] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

means for an individual to establish (subject to limited restrictions) within 40 days[9] what data is held about them and to seek correction or deletion where this may be necessary."

It is a demonstration of FB-I's acceptance and adherence to this requirement that in Chapter 4 of its Update Report to this Office it has fully restated this position.

Recommendation: If identifiable personal data is held in relation to a user or non-user, it must be provided in response to an access request within 40 days, in the absence of a statutory exemption

This is an issue which has captured significant attention due to the some 40,000 access requests received by FB-I over a very short period in October 2011. FB-I continued to receive access requests in the intervening period but at a much lower level.

As indicated in the December Report, the receipt of such a volume of access requests would provide a difficulty for any organisation to provide the personal data held on the requester within 40 days of receipt. FB-I however was in a position that many organisations would not be in whereby it was able to draw upon its engineering resources and in conjunction with this Office identified a suite of avenues to ensure that requesters received their personal data. The agreed upon goal was that wherever possible the data in question should be available to the user without having to make a formal access request. Therefore personal data is available to individual members of FB-I through (i) their own account, (ii) their Activity Log which provides a detailed description and ability to interact and control all their actions on the site, (iii) a download tool which provides additional data which users are typically interested in and (iv) what is termed an expanded archive that provides more detailed information which many users are not seeking to access. FB-I has indicated that it has made the data available through various channels due, in part, to what it terms limitations in the platform infrastructure that underlies the operation of the download tools. FB-I is therefore not able to make every piece of data available by means of the download tools. As this issue only crystallised after the on-site visit we were not in a position to fully assess it. In any case, in terms of access to personal data, as long as the data is available to the user in their account, their Activity log, the download tool or the expanded archive we are satisfied that their right of access is met.

The following FAQ drawn up by FB-I in consultation with this Office provides detailed information to individuals on how to access their personal data from FB-I
https://www.facebook.com/help/?page=116481065103985

The breakdown between the availability of information via the Activity Log, the Download Tool and the Expanded Archive are detailed here
https://www.facebook.com/help/326826564067688

This Office once again during the on-site review sought to ensure that any personal data which was processed by FB-I and which was held in a format that allowed identification of an individual or which related to an individual user was retrievable in response to an access request would be made available to users through the various avenues outlined above. In

[9] Section 4 of the Data Protection Acts

doing so we examined FB-I's various holdings of data as outlined in the updated Technical Analysis Report and in response to specific complaints received accessed individual user account information and examined all personal data held and accessible in relation to specific individuals. At the time of writing the only data which this Office considers to be personal data which is processed by FB-I and not available to individuals is the metadata associated with uploaded photographs (see section 2.2 of the Technical Analysis Report). This material will be added to the Expanded Archive by the end of October. FB-I also holds log data in the logging database Hive, which may include personal data; however, this data cannot be efficiently retrieved per user.

We are satisfied that FB-I has made the efforts envisaged by the Data Protection Acts to ensure that personal data held in relation to individual users is made available to them within the statutory time period. This, of course, is an ongoing obligation as new services and features are introduced on the site and therefore we expect that FB-I will continue to ensure that this obligation is met in such circumstances and that allowing access to all ensuing personal data is written into the relevant product specification in all cases. With the exception of the photograph metadata we are satisfied that all uses are now receiving access to their personal data held by FB-I in a manner that complies fully with the obligations placed under FB-I by Sections 3 and 4 of the Data Protection Acts.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	TARGET IMPLEMENTATION DATE	STATUS
Access Requests	If identifiable personal data is held in relation to a user or non-user, it must be provided in response to an access request within 40 days, in the absence of a statutory exemption	In line with the schedule in relation to availability from the user's profile, their activity log and the download tool. Data will be added to the various tools in phases, beginning in January 2012.	Satisfactory response from FB-I with the exception of uploaded photo metadata which will be available from the end of October.

2.4 Retention

As noted in the December Audit, the requirement to delete or effectively anonymise personal data after the purpose for which it was obtained has ceased is one of the more complex issues which frequently arises in audits and investigations conducted by this Office. We consistently find that the concept is often not well understood and even where it is understood there can be a substantial disconnect between a policy and effective implementation of the retention periods outlined in that policy. We also highlighted that it was perhaps unsurprising therefore that Facebook as still a relatively young company had not yet, as of the date of our audit, fully considered and implemented a retention policy.

The audit therefore provided an opportunity to agree with FB-I on the most appropriate retention periods for the classes of data which it holds. Such retention periods can clearly take account of the legitimate interests of an organisation to process data in line with the services it provides.

Recommendation: The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved.
Recommendation: Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis.

Individual deletion of specific items of data associated with a user perhaps go to the core of the need to identify an appropriate balance between data protection views as to what would be acceptable periods to hold personal data that would meet the requirement to only hold it for as long as is necessary and the desire on the part of FB-I to serve what it perceives to be its users' needs. FB-I retains friend requests and tags after a user has removed them for the reason that it is seeking to protect the user from re-tagging, re-poking, and re-friending. Following extensive engagement, this Office and FB-I agreed that user control in this area could be extended so as to enable users to delete such items on a per-item basis. Such deletion may remove some of the protections and functionality which retaining this information provided to an individual user. From the Activity Log, where this data is displayed, users can now delete the data if they so wish. In this way FB-I has also clarified to users at the time they are taking an action whether that action will cause the item to be deleted or removed. Where it is only removed there is an ability to subsequently delete it via the Activity Log as described above.

We also confirmed that in a situation where both the sender and recipient of a message or chat on the site deletes an individual message that it is not retained in any form and is deleted in line with the process outlined in the Technical Analysis Report.

Users had a pre-existing ability to delete photographs on a per item basis and the Technical Analysis Report comprehensively deals with issues around the Akamai cache where a photo is deleted and the actual process for deleting photographs when a user selects that option or as part of an account deletion is outlined at Section 1.9.2.3 of that Report. This analysis highlighted an issue of concern to this Office in that FB-I, in response to the fact that images could be deleted in error and then lost, has lengthened what is known as the 30 day compaction period by up to another 30 days so that images deleted on day one of that period may be stored for a total of 59 days after the user has selected the delete option, exceeding the 40-day deletion timeframe FB-I have met with respect to most other personal data. FB-I state that it cannot nor does it process these photos while marked for deletion unless they need to be recovered. As such, it views this as the (sole) backup available for this content. We accept that this was unintended by FB-I in response to a genuine recovery issue to potentially hold the data for longer than 40 days in some cases but we expect FB-I to provide proposals for a modified approach to recovery in this area that addresses these

concerns. The same approach will also need to be applied to images which are marked for deletion as part of an account deletion process.

Recommendation: Users must be provided with a means to exercise more control over their addition to Groups FB-I has agreed that it will no longer be possible for a user to be shown as being a member of a group without that user's consent. A user who receives an invitation to join a group will not be shown as being a member until s/he visits the group and will be given an easy method of leaving the group

In response to this recommendation, FB-I changed the way users add their friends to Groups. Previously, any user could add a friend to a Group, and the story that would go into the newsfeed of their friends would be that user A added their friend (user B) to a group. Also any other friend viewing that group would see user B listed as a member even though they had taken no positive or genitive step in relation to the Group. Now, when User A invites User B to Group C, the story that appears in the newsfeeds of their friends is that User A invited User B to join Group C. Until User B visits Group C and has the opportunity to leave the Group, to members of and visitors to Group C, it only appears that User B was invited to the Group. In this way, an inference cannot be drawn that User B has taken an affirmative step to join Group C simply because User B was invited. We are satisfied that this resolves the issue and we have received no further complaints in relation to this feature since those received last year.

Recommendation: FB-I will comply with requirements in relation to retention where the company no longer has a need for the data in relation to the purposes for which it was provided or received. Specifically it will:

1. For people who are not Facebook users or who are Facebook users in a logged out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com.

2. For all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin.

As highlighted in the advertising section of the report, FB-I informed this Office in December 2011 that due to what is termed a litigation hold in the US arising from a class action that could have potentially worldwide applicability for class members that it was unable to delete the data or cease the collection practices in the above areas. It had however segregated the data in line with the retention periods agreed with this Office in relation to such data. This was confirmed by our technical analysis.

Since then, Facebook has been relieved of this obligation and therefore, FB-I will be deleting such stored data. Due to what it states is the complexity of isolating the EU-specific data from all of the data, FB-I expects the deletion process to take several months. This Office will check on FB-I's progress and confirm that deletion has occurred. As this clarification has emerged only recently we do not yet have a precise time period for deletion but expect to receive this from FB-I within two weeks.

In the normal course of events, where data has not been segregated due to the litigation hold, FB-I report that social plugin impression logs for non-users and non-logged in users are deleted after 10 days. In relation to logged-in users, such logs are deleted after 60 days. This was confirmed by a code review.

3. Anonymise all search data on the site within six months
FB-I in its update report has indicated as follows **"**During the audit in December 2011, FB-I proposed a retention policy of six months for user-identifiable search logs. FB-I has begun anonymizing historical search logs. Since that time, FB-I has determined that historical user-identifiable search queries, as opposed to logs, are necessary to improve and deliver to users the ability to search effectively on Facebook. In the alternative to a set retention period for such queries, Facebook will give users control over the retention of their search query data by making their queries visible in the Activity Log, from which users may delete queries, both on an individual basis, or all at once."

FB-I has therefore begun deleting user identifiable search logs but wishes to retain the individual query terms themselves for reasons it has outlined extensively to this Office. This Office accepts, in good faith, that FB-I accepted our recommendation in this area without fully considering the potential implications on how it provides its services to users. However, this Office engaged in extensive and intensive discussions with FB-I to identify ways to give users further control over their search data. Following on from these discussions, FB-I identified, and agreed to introduce, a prominent feature into the user Activity Log where a user can delete if they so wish all of their historic search terms of individual search terms. The feature is listed at 5.4 of the FB-I Update Report. This transparency and control provided to users together with the deletion of search logs provides for appropriate implementation of the recommendation as made by this Office.

4. Anonymise all ad click data after 2 years
This recommendation is implemented except in relation to financial data.

5. Significantly shorten the retention period for log-in information to a period which was agreed with this Office
This recommendation is implemented.

Recommendation: There is not currently sufficient information in the Data Use Policy to educate users that login activity from different browsers across different machines and devices is recorded.
Appropriate additional language was included in the data use policy to highlight this handling of data to users:

"We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby."

Recommendation: Data held in relation to inactive or de-activated accounts must be subject to a retention policy

A detailed analysis of this issue is contained at section 1.9.1 of the Technical Analysis Report. This Office in line with its normal approach in this area had pushed FB-I to set a retention policy for inactive (where the user had simply not returned to the account after their last use) and deactivated(where the user had taken a positive step to deactivate as opposed to delete their account) accounts. In this respect, we adopted our normal approach which was to challenge a data controller to set a retention period which ensured that personal data was not retained for accounts which could not reasonably be believed based on statistical analysis to be likely to ever be required by a user again. The firm belief of this Office was that users who had not sought to access Facebook for periods over two years would in fact not return to the site and therefore such accounts where there was no activity at least for this period and perhaps an even shorter period could be safely deleted by Facebook without deleting data that a user may otherwise wish to access. Prior to the audit, FB-I conducted an analysis at the request of this Office which indicated that in fact users were returning to the site after lengthy periods of time of inactivity. As outlined in the Technical Analysis Report, in order to assess this FB-I was asked to provide data and the relevant account information in relation all accounts which were reactivated from an inactive or deactivated status having lain unused for three years or more on 1 July 2012. In all over 12,000 such accounts were stated to be reactivated on that date. This Office studied approximately 10 of such accounts on 13 July 2012 and confirmed that these accounts had been genuinely reactivated, as opposed to simply being hijacked by malicious programmes etc. Accounts from users situated in the US, the UK, France, Germany and the Netherlands were chosen and all such accounts indicated activity by the user.

In such circumstances it is not considered appropriate at present to require FB-I to institute a fixed retention policy for inactive or deactivated accounts as to do so would clearly result in deletion of data in a not insignificant number of cases where the user in fact would have returned to the site which would be inappropriate. The matter, of course, must be kept under review as there will clearly be a period when Facebook further matures where users after a substantial period of inactivity do not return to the site.

In the meantime, a final issue to be addressed is what steps can be taken to empower those former users with either an inactive or deactivated account who may not wish for it to be retained and would welcome guidance or assistance in deleting the relevant information. In this respect, FB-I has agreed to continue to examine options to contact such individuals and as a first step will instigate a mechanism where after one year of not logging into Facebook, FB-I will notify the user that his or her account will be put into a state of deactivation. That communication will also inform users of the means to delete their account should they so wish. In this way, the account will not be visible on Facebook. Furthermore, FB-I will not use personal information from accounts that have been deactivated or are inactive for more than a year for ad-targeting purposes. This does not include use of such accounts for analysis in aggregate form, such as to analyze patterns around deactivation and inactivity, as mentioned below; to send notifications about activity on the account that the user has chosen to receive; or to conduct database management and upgrades. It has also agreed to an annual communication to users with deactivated accounts to advise them of their options in relation to their account including deletion. As well, FB-I will provide a means to be agreed with this

Office within four weeks for individuals to check whether they have an old account on Facebook and recover it, if so, in order to continue using it, delete it, or deactivate it. Finally, FB-I will re-evaluate its policy regularly, especially as the service gets older and it is able to analyze patterns around deactivation and inactivity. FB-I also agreed to a retention policy for accounts that it disables for violations of its terms. When an account is not needed for security, site integrity, law enforcement, litigation or other legitimate purposes, the disabled account is deleted within 6 months of being disabled. This gives the account holder sufficient time to appeal the decision. FB-I stated that disabled accounts that are needed for the above purposes are stored offline and are not accessible for any other purposes than those. This was not separately verified by this Office on this occasion. However, we will examine at an appropriate opportunity that FB-I is applying the exceptions listed above.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Retention of data	The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved.	Satisfactory response from FB-I
	Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis.	Satisfactory response from FB-I with the exception of an acceptable period for the deletion of images with FB-I requested to provide details of an amended procedure within 4 weeks of this date
	Users must be provided with a means to exercise more control over their addition to Groups	Satisfactory response from FB-I
	Personal data collected must be deleted when the purpose for which it was collected has ceased	Satisfactory response in general from FB-I but subject to a further review from this Office in relation to social plug-in impression data subject that was subject to a litigation hold
	There is not currently sufficient information in the Data Use Policy to educate users that login activity from different browsers across different machines and devices is recorded.	Satisfactory response from FB-I
	We have confirmed that data entered on an incomplete registration is deleted after 30 days	Process changed so this issue no longer arises
	Data held in relation to inactive or de-activated accounts must be subject to a retention policy	We are satisfied with the information provided by FB-I on the justification for the current approach to retention. FB-I to revert within 4 weeks in relation to an appropriate means to contact account holders who have deactivated their accounts or are inactive. Application of exceptions to 6 month deletion period for disabled accounts to be examined

2.5 Cookies / Social Plug-ins

As this is an issue which gave rise to significant concern in the context of the December Audit, we felt it appropriate to re-examine this matter to ensure that the findings and observations contained in that Report and the technical analysis remained valid.

The means by which data is collected from individuals who visit websites with social plug-ins installed has not changed and this is detailed in Section 1.5 of the Technical Analysis Report. The distinction between persons who have never visited Facebook.com, visited it once and not unset their cookies and Facebook users whether logged-in or logged out has also remained.

December Audit Conclusion: We are satisfied that no use is made of data collected via the loading of Facebook social plug-ins on websites for profiling purposes of either users or non-users.
The process for re-testing this issue is outlined at Section 1.5.8 of the Technical Analysis Report. Over 2000 queries served in one particular month to the retained social plug-in data were examined and we were satisfied that no user or non-user data was queried.

Cookies
A detailed re-examination of the use of cookies on Facebook was conducted and is contained in Section 1.5.4 of the Technical Analysis Report. The position as outlined in the December audit has remained broadly the same with the exception of a cookie termed "fr". The purpose of this cookie is outlined at Section 1.5.5.14 of the Technical Analysis Report. As it is a cookie that FB-I is using in order to monitor browsing by users and not for a security purpose, the initial view of this Office is that it falls to be considered as a cookie for which a consent in line with the provisions of Statutory Instrument 336 of 2011 is required. The exact form that such a consent should take is a matter that remains under discussion among enforcement authorities and industry and we expect FB-I to implement whatever that solution is.

It is also clear from public statements made by Facebook and indeed the content of the Update Report that the need to generate revenue from advertising will continue to be a key driver for Facebook and that the innovation that it considers is necessary in this space will in many instances be underpinned by cookie usage which will require detailed analysis in terms of its compliance with data protection law.

Action
FB-I to supply more detailed information to this Office within four week's of today's date on the use of the fr cookie and the consent collected for the cookie that is dropped to support such advertising.

Active Cookie Management
In the December Audit we outlined the need for a continued focus on FB-I taking concrete measures to minimise the possibility of the future collection of unsought data via cookies. FB-I outlined a Cookie Management Framework to assist it in this regard. It was assessed at that time and again on this occasion and confirmed that it continues to operate as described in the December Audit. The analysis is outlined at Section 1.5.6 of the Technical Analysis Report.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Cookies/Social Plug-Ins	We are satisfied that no use is made of data collected via the loading of Facebook social plug-ins on websites for profiling purposes of either users or non-users.	Re-confirmed
	It is not appropriate for Facebook to hold data collected from social plug-ins other than for a very short period and for very limited purposes	Dealt with in Retention Section
	FB-I to supply more detailed information to this Office within four weeks of today's date on the use of the fr cookie and the consent collected for this cookie	Ongoing with FB-I to revert in Four weeks

2.6. Third-Party Apps

This issue was a significant focus of our December Audit. A detailed examination was conducted at that time of the role and use of Apps launched from the Facebook website via a user desktop as opposed to mobile devices. We indicated at that time that we would revert to the issue again with a particular focus on the use of Apps on mobile devices. We have outlined below the analysis conducted. However, in the intervening period the Article 29 Working Party has indicated an intention to bring forward an Opinion on Mobile Applications and in that context this Office decided that it should await the outcome of that Opinion prior to reaching definitive conclusions in this area.

Recommendation: 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 sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications

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 a 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.

Facebook's introduction of an App Centre, while driven by a desire no doubt to encourage users to deepen their engagement with apps, provided an opportunity to standardise the user experience in relation to privacy and the apps use of their information. In Chapter 7 of the FBI Update Report it is indicated that "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."

As outlined in the section on the Privacy Policy/Data Use Policy, the use made by apps of user information is highlighted at the request of this Office as one of the key issues in the initial user education so that users can begin to understand the uses made by applications which they install and which are indeed installed by their friends.

We would consider that the above developments have provided a means for users to exercise choice based on clear information prior to taking a decision to install an app.

Recommendation: 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
The audience selector that is presented to the user before they add an app governs who, if anyone, will see that the user has added the app, as well as who, if anyone, will see activity the app posts to the user's timeline. We are satisfied that this effectively implements the recommendation made.

Recommendation: 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.
The privacy policy link and the ability to report and block an app are now available from the permissions screen. While it is disappointing that there is no explicit encouragement to read the app's privacy policy it is suitably placed to encourage such an action by a user who wishes to do so.

Recommendation: As the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live.
As outlined in our December Report, the ability for a user to read a privacy policy prior to installing an app is seen as a minimum requirement for empowering users. We were pleased therefore 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. It has stated that as with many complex technological tasks, there is a period of time during which FB-I experiences bugs that it must fix. In this case, the bugs have resulted in unwanted results of disabling compliant apps. FB-I expects the tool to be running again by the beginning of October.

The results from the tool are examined by the Platform Operations team who then take appropriate action to ensure developer adherence for the requirement for a working privacy policy link. This is accordingly a matter that will have to be re-examined by our Office when the tool is working in the manner envisaged.

Conclusion: We verified that it 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.

We re-examined this conclusion and have confirmed that the position is unchanged. This is outlined at Section 1.4.4. of the Technical Analysis Report.

Recommendation: 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. However, it should be made easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way at present to manage this is to turn off all apps via a user's privacy settings but this also prevents the user from using apps themselves.
This Office had anticipated that FB-I would 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. FB-I has indicated that the use of Apps is highlighted in the new user education flow which together with the highlighting of how to manage privacy settings during the privacy tour, now directs users to their app settings, where they can choose what private data, if any, can be available to apps their friends use.

We consider therefore that FB-I should revisit this issue with a view to providing more granular choice and control to their users in this area.

Recommendation: We have identified that the authorisation token granted to an application could be transferred between applications to potentially allow a second application to access information which the user had not granted by way of the token granted to the first application. While this is a limited risk we recommend that FB-I bring forward a solution that addresses the concerns outlined. 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 the authorisation tokens provided by it.
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--operation-developer-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.

Recommendation: We do not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. We do note however the proactive monitoring and action against apps which breach platform policies. However, 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 from accessing user information other than where the user has granted an appropriate permission.

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.

Instant Personalisation

This new feature for Apps was raised by FB-I with this Office prior to the Audit. FB-I routinely seeks the input of this Office prior to launching new features and services which may use user data in a manner that could give rise to user queries. This Office encourages FB-I to do so as to ensure that new features and services launched in the EU take account of data protection requirements before launch. As detailed in the Compliance Management/Governance Section it would be our preference for such considerations to be built in from the earliest possible stage of development. The outcome of that engagement which is detailed at Section 7.7 of the FB-I Update Report is that user's navigating to Apps for which instant personalisation is enabled are displayed in each case with a prominent notice on the top of the page that allows the user to make an immediate choice as to whether they wish to continue to use the app or not. If they choose not to, this will disable the application and remove from the application the basic information that was provided under the instant personalisation feature.

Mobile Applications

The screen available to users when installing apps via the Facebook mobile application are contained at Section 7.6 of the FB-I Update Report. As detailed in the Technical Analysis Report, tests were carried out using Android and iPhone devices to assess the usability of certain features. The initial conclusion of this Office, which is likely not unexpected, is that the mobile environment brings with it significant constraints for a user seeking to make informed choices for the use of their information within applications. As an example the permissions screen when loading an application on Facebook from within the Android Marketplace does not contain within the immediately visible information the link to the app's privacy policy. A user must select "view more". Of course even if a user manages to launch the privacy policy it will likely not be overly accessible on a mobile device. These are

not matters that are immediately within FB-I's control but do serve to highlight the difficulties of the space.

As stated at the outset, this Office will await the outcome of the work underway within the Article 29 Working Party on this issue. As a member of the Technology Sub-Group which will prepare this work we will seek to play an active part so as to ensure that our experience in this area is of benefit to the analysis. We will also subsequent to the finalisation of that work engage with FB-I to ensure that relevant best practice recommendations are implemented where not already in place.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Third Party Apps	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 sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications	Satisfactory response from FB-I
	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	Satisfactory response from FB-I
	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.	Satisfactory response from FB-I
	As the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live.	Due to bug issues not operational at present and therefore will be re-examined when operational
	We verified that it 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.	Re-confirmed
	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. However, it should be made easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way at present to manage this is to turn off all apps via a user's privacy settings but this also prevents the user from using apps themselves.	FB-I should re-examine providing choice to their users short of turning off the ability to use Apps altogether
	We have identified that the authorisation token	Satisfactory response from FB-I

	granted to an application could be transferred between applications to potentially allow a second application to access information which the user had not granted by way of the token granted to the first application. While this is a limited risk we recommend that FB-I bring forward a solution that addresses the concerns outlined. 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 the authorisation tokens provided by it.	
	We do not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. We do note however the proactive monitoring and action against apps which breach platform policies. However, 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 from accessing user information other than where the user has granted an appropriate permission.	Satisfactory response from FB-I

2.7 Disclosures to Third Parties

During the December Audit we conducted a detailed analysis of FB-I's approach to dealing with requests from law enforcement for access to user data and assessed the legal basis under which such requests are processed under Irish Data Protection law.

In that Report we indicated that "Under Section 8(b) of the Acts, FB-I is enabled to provide personal data following a lawful request if it is satisfied that to not do so could prejudice the prevention, detection or investigation of an offence. Additionally under Section 8(d), a data controller is enabled to provide personal data if it is required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property. These would appear to be the most relevant considerations for FB-I when responding to lawful requests."

In the context of the December Audit we examined five randomly chosen requests from law enforcement and concluded that FB-I had processed such requests appropriately. Given the sensitivity of this issue and taking account of input from colleague data protection authorities where a particular concern had arisen in relation to the disclosure of IP addresses in response to such queries, this Office again examined a random sample of requests received by FB-I in the days before 10-13 July 2012. We were joined once again by the Facebook Chief Security Officer for this examination. A sample of the requests examined is re-produced in the attached table:

Requesting Authority	**Basis of Request**	**Information Sought**	**Outcome**
French National Police	Person suspected of possession of	Subscriber information and IP address information	Granted

	child pornography		
German State Police from Bavaria	Missing Child	Log-in and IP address details	Granted
Italian Postal Police	Defamation Case	IP Address Logs	Not Granted
Portuguese Public Prosecutor	Domestic Violence Case	IP Address Logs	Not Granted due to vague nature of request
UK Police Constabulary(using SPOC form)	Kidnapping Case	Log-in and contact information	Granted
Irish Police Force	Threats made against a police officer	Subscriber information and IP logs	Granted

All of the requests that were granted met the conditions outlined in Sections 8(b) & 8(d) of the Data Protection Acts. We were also satisfied that FB-I is appropriately assessing requests and either seeking additional information or justification where it has concerns or is refusing such requests.

Recommendation: The current Single Point of Contact (SPOC) arrangements with law enforcement authorities when making requests for user data should be further strengthened by a requirement for all such requests to be signed-off or validated by a designated officer of a senior rank and for this to be recordable in the request. We also recommend that the standard form used require all requesting entities to fully complete the section as to why the requested user data is sought so as to ensure that FB-I when responding can form a good faith belief that such provision of data is necessary as required by its Privacy Policy. FB-I should also re-examine its privacy policy to ensure that the current information provided is consistent with its actual approach in this area.

Facebook has produced detailed guidance for law enforcement agencies in relation to requests for user data which are available on the site.[10] These guidelines make clear the responsibility of FB-I for processing requests in the EU.

The Law Enforcement Response Team (LERT) in Dublin has also been expanded. To ensure that the members of the team can appropriately assess privacy and data protection impacts from requests, there is now a requirement for all staff members in the Team to have attained an appropriate privacy/data protection certification. The LERT manager is a member of the cross-functional data protection compliance team managed by the Head of Data Protection and escalates any unusual requests, as well as monitors his team for data protection compliance.

In its Update Report, FB-I has outlined the steps it has taken to comply with the recommendations as follows "Facebook has further developed and strengthened the SPOC arrangements with the UK and Irish authorities and has actively promoted possible SPOC arrangements with other countries. In particular, Facebook has conducted training and outreach with the UK SPOC authorities to reinforce the legal and operational requirements to properly submit law enforcement requests to Facebook, including the importance of signed

[10] https://www.facebook.com/safety/groups/law/guidelines

requests that provide details about the basis of the request to ensure compliance with local law and Facebook's terms. Additionally, Facebook has encouraged law enforcement authorities throughout the EU to adopt a SPOC model in light of the mutual operational advantages of the SPOC system. These outreach efforts have been favorably received by law enforcement authorities in a number of countries and Facebook will continue to work to formalize processes to support the SPOC model where possible."

We are satisfied that FB-I is making reasonable efforts to encourage law enforcement authorities to use the SPOC form when making requests but it is clear that such use has not yet become standardised. We acknowledge that this is an ongoing process, which requires the mutual engagement of FB-I and local law enforcement. The benefits of the use of a standardised approach for all are outlined in our recommendation and we would expect that FB-I will continue in its ongoing efforts to encourage law enforcement authorities to use the SPOC form.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Disclosures to Third Parties	The current Single Point of Contact arrangements with law enforcement authorities when making requests for user data should be further strengthened by a requirement for all such requests to be signed-off or validated by a designated officer of a senior rank and for this to be recordable in the request. We also recommend that the standard form used require all requesting entities to fully complete the section as to why the requested user data is sought so as to ensure that FB-I when responding can form a good faith belief that such provision of data is necessary as required by its privacy policy. FB-I should also re-examine its privacy policy to ensure that the current information provided is consistent with its actual approach in this area.	Satisfactory response from FB-I

2.8 Facial Recognition/Tag Suggest

As explained in the December Audit: "When a user uploads a photo album, photos containing the same person are automatically grouped together by Facebook. Facebook then suggests names for friends in some of these groups to help save the user time creating and sharing albums."

In March, the Article 29 Working Party published an Opinion 02/2012 on facial recognition in online and mobile services[11]. This Opinion was directly applicable to how Facebook provides its Tag Suggest/Facial Recognition feature.

[11] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Recommendation: FB-I should have handled the implementation of this feature in a more appropriate manner and we recommended that it take additional steps from a best practice perspective to ensure the consent collected from users for this feature can be relied upon

FB-I agreed with this Office in response to this recommendation that it would "provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings."

It will be noted that this agreement was reached with FB-I prior to the Article 29 Opinion on the use of facial recognition generally in online services.

FB-I in its Update Report to this Office highlighted that it had now provided two sets of notice to users of its tag suggestions feature and had updated its Data Use Policy with a link to a more detailed description of tag suggestions. It also emphasised that prior to the Audit:

- Each user was given prominent notice of the new feature on her/his FB-I home page. The notice appeared at least three times;

- The notice provided a link to further information on the feature, including how to disable it; and

- The then-current method of disabling the feature was modified to further simplify it.

It further stressed that in specific response to the December Audit, between early January and July 2012, FB-I ran a banner on the user's homepage, which appeared at the top of the page when the user logged in. If the user interacted with the banner by selecting either option presented, then it disappeared for the user. If the user did not interact with it, then it appeared twice more for a total of three displays on the next successive log-ins. Before making a selection, more detail about how the feature works appeared behind a "Learn More" link. If the user clicked "Edit Settings", they would be taken to their privacy settings page where they could turn off the feature.

FB-I has highlighted that it has also updated its Data Use Policy and is providing users with access to the biometric template in the user's expanded archive.

In relation to existing users on the site, FB-I complied with the recommendations contained in the December Audit Report. The issue of how to capture an appropriate consent from new users was under active discussion with FB-I in the early part of the year, however as this Office was aware that the Article 29 Working Party was bringing forward its Opinion in this area it was decided to await its publication and further discuss the matter at that time.

Following publication this Office made clear to FB-I that we expected it to comply with the relevant recommendations in the Opinion. FB-I immediately undertook to do so and an outline mechanism to capture an appropriate consent from new users at a time that was most relevant such as when they were first tagged in a picture that they did not remove was agreed. The mechanism required the user to make a selection one way or the other to either use Tag Suggest or not and if they decided to not use the service, it would be turned off by simply selecting the option on screen. Relevant information was to be provided on screen in relation to the service and its use of biometrics.

This Office was also aware from both parties that the Hamburg Data Protection Authority was in contact with FB-I/Facebook on this issue. We had welcomed the previous decision the Hamburg DPA had taken to suspend a proposed action against Facebook Inc in relation to the Tag Suggest feature pending the completion of our negotiations with FB-I in the context of the re-audit.

We are aware that the Hamburg DPA took a decision to re-commence their suspended action which is directed at Facebook Inc. While FB-I has met the agreement with this Office as outlined in our audit report, we were obviously conscious of the concerns expressed. Therefore we engaged in detailed discussion with FB-I to identify options towards a satisfactory outcome.

Both this Office and FB-I were conscious however of the passage of time and therefore pending their conclusion, FB-I as a gesture of goodwill in August suspended the Tag Suggest feature for all EEA users who had joined since 1 July (it was possible to back-date it to this date due to a suspension for technical upgrade reasons around that time).

As outlined in the December Audit, this Office is obligated to take account of Irish case law in relation to the use of biometrics which has not considered that the use of biometrics requires explicit consent. Therefore in a situation where FB-I has implemented the recommendations outlined by this Office and has suspended the service for new users with effect from 1 July 2012 until a holistic solution can be found, this Office does not consider that there is any basis for action by it against FB-I to re-consent previously enrolled users.

Nevertheless, as in many areas during this audit we are acutely aware that it is incumbent upon us to take account of the views and opinions of colleague data protection authorities in other Member States who although they may have no direct jurisdiction over Facebook unlike the direct jurisdiction which this Office has over FB-I, do obviously have a right to represent the views of the residents of their countries or regions who use Facebook. Therefore taking account of the views of this Office on this matter, we are encouraged that FB-I notwithstanding any views it may have on the precise legal requirements that apply has decided to adopt a best practice approach in this area and has agreed to delete all existing biometric templates of EU users by October 15 at the latest. This will be verified by this Office. It has also agreed not to resume building templates until or unless it gives new notice and obtains consent from all EU users in a form consistent with this Office's guidance.

Conclusion: We have confirmed that the function used to delete the user's facial profile is invoked when the user disables "tag suggestions".

We have re-confirmed that disabling the tag Suggest feature deletes the individual user template. This is outlined at Section 2.8 of the Technical Analysis Report.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	STATUS
Facial Recognition/Tag Suggest	FB-I should have handled the implementation of this feature in a more appropriate manner and we recommended that it take additional steps from a best practice perspective to ensure the consent collected from users for this feature can be relied upon	FB-I will provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings. FB-I will discuss with this Office any plans to extend tag suggest to allow suggestions beyond confirmed Friends in advance of doing so.	Implemented. FB-I has also agreed to delete collected templates for EU uses by 15 October and to agree a process for collecting consent with this Office if it chooses to provide the feature to EU users again.
	We have confirmed that the function used to delete the user's facial profile is invoked when the user disables "tag suggestions".		Re-confirmed

2.9 Data Security

In our December Audit we examined FB-I's approach to data security. While noting that it was clear that the procedures and policies implemented by FB-I had appeared to have served the site well, there were a number of issues which we identified for further analysis and consideration in the re-audit and therefore significant time on the re-audit was focused on assessing FB-I's approach to data security with a particular focus on the principle of "need to know" access to personal data. This is clearly an important issue in relation to an organisation which has access to some 1 billion user accounts and information – a scale of access that is unprecedented and which therefore calls for a best practice approach to data security.

We did not seek to assess FB-I's approach to preventing large scale intrusion attacks or other attempts to inappropriately access the system as it is clear to this Office that this is a key

focus of FB-I and the record of FB-I in this area thus far did not justify a focus on this particular aspect.

The detailed examination which was undertaken is outlined at Section 1.3.2 of the Technical Analysis Report.

Recommendation: Many policies and procedures that are in operation are not formally documented. This should be remedied.
FB-I supplied a number of polices in relation to internal access to personal data and the procedures and practices in place for granting and removing such access as well as ensuring that all such access when granted is appropriate.

Recommendation: We are satisfied that FB-I does have in place an appropriate framework to ensure that all access to user data is on a need to know basis. However, we recommended that FB-I expand its monitoring to ensure that there can be no employee abuse through inappropriate password resets of a user's account
FB-I implemented this recommendation during January 2012

Recommendation: We were concerned that the tools in place for ensuring that staff were authorised to only access user data on a strictly necessary basis were not as role specific as we would have wished
FB-I has enhanced its tools and procedures in this area to a level that is acceptable to this Office. It has in place strict approvals for employee access to particular tools, peer review of such approvals and the withdrawal of such access after a specified period or where no actual use of the access provided has taken place. This is supplemented by extensive logging and monitoring of employee access which is constantly refined to ensure that, in so far as is possible, that patterns of inappropriate access are detected. This Office is therefore satisfied that FB-I has in place an appropriate framework for ensuring that access to user data is strictly controlled and monitored.

We note that FB-I is in the process of further enhancing its approach in this area by moving to a model of approved access to specific user accounts in response to specific issues arising. This should further assist to restrict the potential for inappropriate access to user data on the site.

December Audit Conclusion: We are satisfied that there is no realistic security threat to a user photo from their upload to Akamai. We are also satisfied that there is no realistic threat to a deleted image
The position established on this issue is outlined at Section 1.6 of the Technical Analysis Report. There is no realistic threat in this area.

December Audit Conclusion: We believe that current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data via "screen scraping" while allowing the service to be effectively provided to legitimate users.
The position on this issue is unchanged.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Security	Many policies and procedures that are in operation are not formally documented. This should be remedied.	Satisfactory response from FB-I
	We are satisfied that FB-I does have in place an appropriate framework to ensure that all access to user data is on a need to know basis. However, we recommended that FB-I expand its monitoring to ensure that there can be no employee abuse through inappropriate password resets of a user's account	Satisfactory response from FB-I
	We were concerned that the tools in place for ensuring that staff were authorised to only access user data on a strictly necessary basis were not as role specific as we would have wished.	Satisfactory response from FB-I
	We are satisfied that there is no realistic security threat to a user photo from their upload to Akamai. We are also satisfied that there is no realistic threat to a deleted image	Position as stated in December Audit
	We believe that current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data via "screen scraping" while allowing the service to be effectively provided to legitimate users.	Position as stated in December Audit

2.10 Deletion of Accounts

As outlined in the December Audit, the Data Protection Acts provide a right to seek deletion of personal data held by a data controller which must be complied with other than where a data controller can demonstrate legitimate interests for the continued retention of the data in question. That clearly would not apply in relation to requests received, in the normal course, from Facebook account-holders. Deletion requests therefore must be complied with by FB-I within 40 days of receiving the request further to the provisions of Section 6 of the Data Protection Acts. FB-I indicates that it has spent considerable time and resources over the past year of our engagement in the context of the Audit to try to reach a situation where it can irrevocably delete personal data following an account deletion request.

The process for requesting the deletion of a Facebook account as opposed to deactivation has remained largely as outlined in the December Report. Where deletion is sought accounts are immediately removed from the site and placed in a deactivated state pending deletion for a period of 14 days to allow the user to change their minds. According to FB-I, 40% of users who make deletion requests change their mind within this 14 day period. After the 14 days an account is placed in a queue for deletion which ensures that the account information is effectively deleted within a further 24 hours.[12] In case of deletion errors for instance where the wrong information may be deleted, within a further 14 days from the initial 14 day

[12] FB-I state the median is 6 hours, but some accounts take several days due to databases being down, corruption of data that must be corrected, and extremely large accounts

deletion period there is a possibility for a manual restoration of an account. The process however is very labour intensive requiring extensive engineering time and we would not consider that it would be used other than in exceptional circumstances. In any case, the account level information can be considered to be effectively deleted within 28 days of the making of a request.

The challenges which FB-I has faced around verifiable deletion of personal data associated with accounts relate to the volumes of information held in various databases and log files. Efficiently and comprehensively identifying all information relating to an account being deleted is technically challenging. These issues are addressed in detail in Section 1.9 of the Technical Analysis report.

Since the December Audit, FB-I indicates that it has continued to improve its account deletion framework and what it describes as the monumental task of anonymizing/delinking historical log data. The process of delinking/anonymizing logs, which was highlighted in the December Audit as needing additional time to complete, is now stated to be complete

Recommendation: There must be a robust process in place to irrevocably delete user accounts and data upon request within 40 days of receipt of the request (not applicable to back-up data within this period.)
It is clear that FB-I has extended considerable time and resources to ensure that where a user requests deletion of an account that it takes place in a timely fashion taking account of the 40-day period specified in the Data Protection Acts, which may apply to some requests for deletion. The challenges of effectively deleting all personal data held in various database and log file holdings are addressed in detail in the Technical Analysis Report.

In this respect, when an account is deleted we do not believe that it is possible to link data that has been de-identified with that account in any way. An issue of concern however to this Office is the status of the 90 days worth of log data that have not been de-identified yet at the point when the account is deleted. The preliminary view of this Office is that it may be possible that there is personally identifying content left until the entire 90 days of logs from the date the user requested account deletion has been de-identified. Therefore we are requesting further clarity from FB-I on this issue within four weeks from today's date so as to further assess this complex issue.

Additionally, FB-I found it complex to disassociate one user's data from a group without having knock-on implications on posts within the group. It has highlighted this issue in its updated Data Use Policy but as outlined at Section 1.9 of the Technical Analysis Report it is intended that this issue will be resolved by early 2013 at which point the deletion solution will be retrospectively applied to all previously deleted accounts to ensure that associated group content is also deleted. In the meantime, the content in question is not available on the site.

Outside of these issues and an issue in relation to the deletion of photographs in response to individual delete actions and during account deletion highlighted in the Retention Section of this Report all of which we expect to be resolved or clarified, this Office is satisfied that the

procedures now in place ensure that FB-I is meeting its statutory requirement to delete all personal data held in an account within 40 days of a request for such deletion

Deletion of individual items from Activity Log
As noted earlier in this Report, a user's activity log provides them with a means to control individual items of content associated with their Facebook account. This control also allows for the deletion of individual items of content. As previous concern had arisen as to whether items marked for removal were in fact deleted, specific items were selected from an Activity Log and the delete option was selected. We assessed whether such items were in fact deleted. This was done by way of functional testing using DYI to verify what had been deleted, and it was confirmed that the deletion framework applied to account information is also applied to such data items.

FB-I has also stated that this inability to perform efficient, per-user queries is also why FB-I cannot today offer download of stored log data in response to subject access requests or in its user-facing Download Your Information (DYI) tools.

It has stated the following "notably, hashing is not used to deidentify user_ids. The reasons are three-fold:

1. The need to perform longitudinal analysis on undeleted accounts prevents the use of a rotating key as is used for datr cookie deidentification.
2. Hashing has no effect on forward lookups. This means that given the user_id of a deleted account, FB-I could just as easily query the hashed user_id as the original user_id. Hashing has not affected any deidentification at all.
3. Hashing is only one-way when there are a very large number of possible inputs. Even though FB-I is a large service with hundreds of million registered accounts, FB-I could easily and efficiently find the original user_id corresponding to a hashed user_id by simply testing each known registered user_id. Assume FB-I has 1 billion such user_ids. A simple laptop computer is capable of computing more than 1.8 million hash operations per second, thus FB-I, using a single laptop computer, could check all 1 billion user ids in less than ten minutes."

Deletion of National ID documents
In case of disputes as to the authenticity of an account on site, FB-I can, in order to make an assessment as to whether an account is an imposter account or genuine, seek a form of national ID from a person to validate their claim to the account. The national ID documents are used to assess picture on the site, birthday supplied and full name. Equally where an account may have been compromised and none of the online remediation techniques succeed then the user can request access by submitting a ticket to FB-I's user operations.

This may require the user to send a copy of a piece of identification (such as a national identity card or passport) to FB-I. The picture of the identification is stored as an attachment to the user's support ticket. From a data protection perspective, there is no reason why FB-I needs to hold such personal data other than for a very short period.

An automated process deletes attachments from tickets that have not been modified for 28 days. A review of the ticketing system was carried out during the audit and a selection of tickets were examined where the user would have been required to send identification to FB-I.

It was noted that all tickets examined that had not been modified for more than 30 days had no attachments remaining. This is consistent with the deletion of attachments by an automated process. From our reviews of the operation of user operations, once a ticket is processed through a queue there is usually no reason for it to be re-opened and therefore in almost all cases the 28 day period will apply immediately from the time that the ticket is processed through the queue.

The code that performs the deletion of the attachments on tickets that have not been modified for more than 28 days was also reviewed and confirmed to operate as described here.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	OUTCOME
Deletion of Accounts	There must be a robust process in place to irrevocably delete user accounts and data upon request within 40 days of receipt of the request (not applicable to back-up data within this period.)	Given the scale of the task, a satisfactory response from FB-I pending resolution or clarification within four weeks on image deletion and log de-identification, with group content to be deleted in early 2013

2.11 Friend Finder

As indicated in our December Audit, the operation of this feature to prompt invitations to non-users had at that time given rise proportionately to the largest number of queries to this Office in relation to how Facebook came to know their friends etc. We therefore subjected this feature to a detailed examination while at the same time noting similar work underway by our colleagues in the Office of the Privacy Commissioner of Canada which we did not wish to replicate.

December Audit Conclusion: We are satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder purposes.

The technical operation of the friend finder and synchronisation feature is described in Sections 1.1. & 1.2 of the Technical Analysis Report. The technical analysis has indicated that FB-I has not altered its use of telephone numbers or other contact details uploaded as part of friend finder and synchronisation.

Recommendation: We recommend that users be made aware that where they choose to synch their contact information from a mobile device, those contact details are transmitted in plain text and are therefore not secure during transmission.

FB-I Commitment: It is not more risky to send data in plain text via the synchronization process than doing so by sending email using an internet email provider that does not support secure connections, which providers do not provide disclosures on security risks. FB-I will have further dialogue in order to work towards reviewing alternatives for reducing risk and addressing them through education or changes in the product.
As outlined at Section 1.2.1 of the Technical Analysis Report, in our December Audit we outlined that the contact information transmitted by the iPhone Facebook application while contact synchronisation was taking place was transmitted in plain text. We also highlighted that secure browsing was not supported on the mobile platform. It has been confirmed as part of the current Audit that communication is encrypted using TLS between Facebook and both the iPhone and Android Facebook applications.

Recommendation: We established that the action of disabling synchronisation does not appear to delete any of the synchronised data. This requires an additional step via the "remove data" button within the app. We recommend that it should be clear to users that disabling synching is not sufficient to remove any previously synched data.
FB-I Commitment: It should be obvious to users that their synchronized data is still there after they disable synching but FB-I will add text to that effect within the app.
Facebook has updated the means by which its mobile applications operate and has removed synching from the latest iPhone app. It simply has contact importer, so everything stays within the app – it's a one-way transfer of contacts – to Facebook. FB-I has undertaken to ensure that the process of syncing in the Android version of its app discloses to users that turning off syncing does not delete synced data from Facebook.

FB-I also reports that when a user removes their uploaded contacts from Facebook, FB-I retains a hashed value of the email addresses in order to prevent reminder emails from being sent to those removed contacts.

Recommendation: We were concerned that the facility whereby businesses could upload up to 5,000 contact email addresses for Page contact purposes created a possibility of the sending of unsolicited email invites by those businesses in contravention of the *e*Privacy law with an associated potential liability for FB-I. We recommended a number of steps to be taken to address this risk
FB-I Commitment: FB-I in response immediately geoblocked the major EU domains so that messages from Pages cannot be sent to the vast majority of EU users or non-users. It will further improve the information and warnings made available to businesses using this facility.
At Chapter 12 of its Update Report, FB-I has indicated that it "already provided numerous protections around its business contact importer product to minimize the risk that EU individuals would receive emails from Page administrators. These measures included: 1) blocking all major EU domains; 2) requiring administrators to check a box affirming that they have consent to send the emails; and 3) prominently displaying a message that alerts Page administrators to the requirement that they comply with all applicable laws, including European laws.

FB-I currently blocks a dynamic list of over 300 Internet domains, which is far over-inclusive and thus significantly reduces the risk that any Page emails will be received by individuals in the EU.

The DPC also advised that any addresses a Page administrator removed from its imported contacts should not be used for friend-finding purposes. In fact, currently, FB-I does not store any of a Page administrator's uploaded contacts and does not use any of such contacts for friend-finding purposes."

The operation of this feature as described by FB-I was comprehensively tested during the re-audit as outlined at Section 2.6 of the Technical Analysis Report and found to be operating as described.

December Audit Conclusion: We confirmed that passwords provided by users for the upload of contact lists for friend-finding purposes are held securely and destroyed
As outlined at Section 1.1.4 of the Technical Analysis Report, the code used to perform this functionality has been re-examined and it has been re-confirmed that the e-mail provider password is stored in memory for the duration of the import task and then discarded.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Friend Finder	We are satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder purposes.	Reconfirmed
	We recommend that users be made aware that where they choose to synch their contact information from a mobile device, those contact details are transmitted in plain text and are therefore not secure during transmission. This is not an issue within Facebook's control but users should nevertheless be made aware when choosing this option.	Data now securely transmitted
	We established that the action of disabling synchronisation does not appear to delete any of the synchronised data. This requires an additional step via the "remove data" button within the app. We recommend that it should be clear to users that disabling synching is not sufficient to remove any previously synched data.	The released version of the iPhone App has addressed this issue. FB-I to revert to this within 4 weeks on the addition of disclosure to the Android version of the app.
	We were concerned that the facility whereby businesses could upload up to 5,000 contact email addresses for Page contact purposes created a possibility of the sending of unsolicited email invites by those businesses in contravention of the *e*Privacy law with an associated potential liability for FB-I. We recommended a number of steps to be taken to address this risk	Satisfactorily addressed by publication of December Audit and re-confirmed
	We confirmed that passwords provided by users for the	Re-confirmed

	upload of contact lists for friend-finding purposes are held securely and destroyed	

2.12 Tagging

The use of Tags was considered in detail in our December Audit. We had sought to understand the use case for Tags and the potential privacy issues that arise from a Tag that is attributed by one friend to another. Tagging a friend notifies that friend that they are so tagged and then they can take various actions in relation to that Tag if they so wish. Placing the name of a person who is not a friend on a Tag does not cause any association to be made. As explained in the December Audit, "A tag can be placed on any object and a name attributed to it. For instance a picture of the Eiffel Tower can be tagged with "Eiffel Tower" or indeed any other tag a user wishes to put on it. The tags themselves as they have no separate logic attaching to them are not associated with a particular user. If however a member tags a picture or a comment, post etc with a tag identifying a friend, an association with the friend is made and they are sent a notification of the tag with an ability to remove it."

Recommendation: There does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it.

We were aware from our discussions during the December Audit that FB-I had detailed reservations over introducing an ability for a user to prevent tagging of them by their friends due largely to the loss of control that would arise for the person. Equally it was FB-I's view that Facebook users fully understood how Tags worked and were interacting with them in a way that illustrated this. In this respect at the request of this Office it provided a breakdown of Tag usage for US based users on a single day in July 2012:

Users tagged = approx 14 million per day
Users rejecting tag = approx 44 thousand per day
Photo tag created = approx 3.7 million per day
Photo tag deleted = approx 830 thousand per day

In its Update Report FB-I stated "As tagging has expanded, FB-I has been sensitive to those users who may want more control over the process. Thus, FB-I offers users: 1) notice of tags; 2) the ability to pre-approve tags before they appear on their timelines; 3) the ability to un-tag; and 4) review tags others add to one's own posts. Furthermore, if a user feels in any way harassed by unwanted tags, the user can block the person, which will prevent that person from being able to tag him or her. And finally, Facebook introduced the ability to remove the record of a removed tag altogether in the user's Activity Log. FB-I believes that it has struck the right balance in terms of product development and user control. "

These figures would indicate that users are interacting in a fully informed way with how tags work in practice. We are also not aware of inappropriate uses of Tags that have not been resolved using the person-to-person tools provided by Facebook in the first instance or by recourse to user operations via a complaint. It will also be noted that we asked FB-I to include Tagging as one of the priority items in the new user/existing user education that is outlined in the Data Use Policy/Consent Section of this Report. Finally and importantly a user

can at anytime now delete a Tag via their Activity Log and the record of the Tag will be irrevocably deleted. Taking account of the above therefore we are not requiring the introduction of an ability to prevent Tagging at this time.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Tagging	There does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it.	Taking account of the various tools available to users to manage Tags and to delete them if they so wish we are not requiring an ability to prevent Tagging at this time.

2.13 Posting on Other Profiles

The ability for Facebook users to be aware in advance of making a post on another user's page what the audience for the post would be was raised in a complaint to this Office. We had discussed the matter in detail with FB-I during the December Audit process and while noting reservations on the part of FB-I we nevertheless felt that there was potential for alternative options to emerge during the audit review phase. The data protection concern was to ensure that an individual has full information when making a post. A difficulty correctly pointed out by FB-I in reply is that it is not possible to reveal personal data (i.e. their privacy settings) about the person on whose page you are posting without running into data protection concerns.

Recommendation: We recommend that FB-I introduce increased functionality to allow a poster to be informed prior to posting how broad an audience will be able to view their post and that they be notified should the settings on that profile be subsequently changed to make a post that was initially restricted available to a broader audience. We recommend the sending of a notification to the poster of any such change with an ability to immediately delete their post if they are unhappy.

The FB-I response on this issue is outlined at Chapter 14 of the Update Report as follows:
"It is important to FB-I that users understand that content they share may, in turn, be shared by others more broadly and, if it is content shared on another user's timeline, will be visible to an audience that may be as wide as "everyone". It is a simple model, and it encourages responsible sharing. Users have the most control over their own timeline. But when a user decides to post on another user's timeline, he or she does so understanding that he or she does not control the visibility of the post. Users who wish to communicate privately can use any one of Facebook's messaging products – messages, emails, or chat.

Furthermore, Facebook already offers users the ability to see the general audience of a user's post on his or her timeline, which means, users who wish to make a comment on that post can see the general audience of the comment, e.g., friends of friends of the user whose timeline it is."

This Office has considered this issue in detail taking account of FB-I's responses and is inclined to the view that if a Facebook user chooses to post on another Facebook user's page that they do not do so with an expectation that the post will be either private or restricted to an audience that they are comfortable with. If a user has a concern about the audience for a post they make or that the audience might be subsequently expanded from say "friends only" to "Public" then there is a simple solution available to them and that is not to post on other user's pages. Each user can fully control the audience for all items on their own page but they cannot have an expectation, at least from a data protection perspective, that they should be able to control the use of information they post on another user's page.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Posting on Other Profiles	We recommend that FB-I introduce increased functionality to allow a poster to be informed prior to posting how broad an audience will be able to view their post and that they be notified should the settings on that profile be subsequently changed to make a post that was initially restricted available to a broader audience. We recommend the sending of a notification to the poster of any such change with an ability to immediately delete their post if they are unhappy.	We are satisfied with the information provided by FB-I on the operation of this function

2.14 Facebook Credits

Recommendation: We are satisfied that FB-I does act as a data controller in the provision of the Facebook Credits service. However, we would consider that it is not fully apparent to users using the service that FB-I is acting as a data controller and that information generated in the context of their use of Facebook Credits is linked to their account. It is recommended that the Data Use Policy be significantly expanded to make clear the actual personal data use taking place in the context of Facebook Credits.

FB-I committed in response to supplement appropriate information to its Data Use Policy and noted that it was launching a privacy policy for its payments systems in approximately six months. It updated its Data Use Policy with additional references to Facebook Credits to make it clearer to users that when they interact with that service that the personal data arising is associated with their account. In addition, FB-I's parent company has begun the process of creating payments-specific privacy terms, and has launched such terms for North American users, available at https://www.facebook.com/payments_terms/privacy.

For European users, FB-I has created a subsidiary, Facebook Payments International Ltd. (FB-PI) FB-PI intends to prepare and launch a payments-specific privacy policy in late 2012 or early 2013.

The Payment Terms associated with the service also make clear that the terms are between FB-PI and EU residents where that is applicable.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Facebook Credits	We are satisfied that FB-I does act as a data controller in the provision of the Facebook Credits service However, we would consider that it is not fully apparent to users using the service that FB-I is acting as a data controller and that information generated in the context of their use of Facebook Credits is linked to their account. It is recommended that the Data Use Policy be significantly expanded to make clear the actual personal data use taking place in the context of Facebook Credits.	Satisfactory response from FB-I pending further clarification emerging from the operation of FB-PI

2.15 Pseudonymous Profiles

The issue of pseudonymous profiles was addressed in detail in the December Audit and was therefore not addressed again in totality. We are aware that the Committee of Ministers to the Member States of the Council of Europe issued a recommendation in April on the protection of human rights with regard to social networking services[13] which has relevance in this area and which we brought to the attention of FB-I.

In the December Audit we made clear that we considered that FB-I had advanced a sufficient rationale for child protection and other reasons for their policy position to require real names on the site and did not consider that from an Irish data protection law perspective that there was sufficient justification as to require that FB-I adopt a different policy.

Subsequent to the December Audit, a colleague data protection authority highlighted an issue that was arising in their country whereby employers were requiring employees to administer Business Pages on Facebook and in doing so the employee was having to reveal their personal Facebook account as a consequence and that in such circumstances Facebook should allow a pseudonymous account for the Business Page on Facebook. FB-I in response clarified that Facebook profiles are personal, not professional, accounts. Businesses and other professionals can set up Pages using the business or professional name. It pointed out that users can use their privacy controls to segment the audiences that see their timelines. For example, a user can create a friend list called “professional contacts” and put all work-related “friends” into that list. The user can then create a friend list called “personal friends” and put all personal friends into that list. Then, when the user wants to post something

[13] https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM

specifically to one or the other, the user simply chooses the appropriate list in the in-line privacy drop-down, which is part of every post.

FB-I has highlighted the following on this issue: "Facebook offers businesses, charities, musical bands, and other non-individuals the ability to set up a Page. See https://www.facebook.com/pages/create.php?ref_type=sitefooter. Pages operate differently from individual timelines, where users must use their real names. Pages are public by default. However, the administrator of the Page must have a separate account, which requires nothing more than an email address. There is no need for a Page administrator to mix professional and personal activity on Facebook. However, if the administrator already has a Facebook account, he or she can use that account as the linked account. This still does not require any mixing at all of the Page and the personal account. The administrator's personal account may hide the fact that he or she is the Page administrator, and, likewise, the Page can hide the identity of the administrator. Facebook requires a linked account in order to have an individual accountable for the Page. For more information, see https://www.facebook.com/help/?faq=217671661585622#How-are-Pages-different-from-personal-timelines? The purpose of a Page is not to be able to interact socially with a pseudonym. If a user wants to communicate differently with different sets of people, he or she can use lists. See https://www.facebook.com/help/?faq=200538509990389#How-do-I-use-lists-to-organize-my-friends? A user can also create custom lists. See https://www.facebook.com/help/?faq=190416214359937#How-do-I-add-friends-to-existing-lists-or-create-a-new-list?. In addition, there is an entire section on Pages in the Help Center. https://www.facebook.com/help/?page=203955942973503&ref=bc. "

It has also emphasised that it does not require that page administrators publicly disclose their identity and does not condone any practice which sees employers forcing employees to disclose their identities, and professional affiliations, on Facebook against their will.

We consider that the specific issue highlighted is not a matter for FB-I. Clearly if an employer is requiring an employee to disclose their personal identity in the context of administering a Page that is a matter for the employee and the employer and relevant laws applicable to such a situation.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION
Pseudonymous Profiles	We consider that FB-I has advanced sufficient justification for child protection and other reasons for their policy of refusing pseudonymous access to its services

2.16 Abuse Reporting

In our December Audit we outlined the measures that FB-I had in place for users and non-uses to report concerns or abuses. On an inherently social and open site such as Facebook, an effective and well resourced means for individuals with concerns to report or take action in relation to those concerns is paramount. This is also very well understood by Facebook which places great importance on ensuring a safe environment for its users.

December Audit Conclusion: We are satisfied that FB-I has appropriate and accessible means in place for users and non-users to report abuse on the site. We are also satisfied from our examination of the User Operations area that FB-I is committed to ensuring it meets its obligations in this respect.

This Office, together with colleague Data Protection Authorities continues to receive complaints and queries from Facebook users and non-users about concerns on the site. The most frequent source of query to this Office in this respect is fake accounts or imposter accounts where the individual complaining is not a member of Facebook and cannot identify the correct means to report the account in question.

Therefore as part of the audit follow-up and review process, we engaged with FB-I regarding the difficulties reported by non-users trying to locate a contact point or appropriate link on Facebook which would allow them to report abuse of some kind such as an imposter pretending to be them. This Office requested that FB-I make the channels under which non-users could report abuse more prominent and accessible.

At the time of the December Audit, if a non-user clicked the **'Help'** link situated in the bottom right hand corner of the homepage of www.facebook.com they were taken to a page which featured an option '***Report Abuse or Policy Violations'*** (this screen was referred to in section 13.6.1 of the December Audit). If this option was clicked the non-user was presented with a list of the types of issues that could be reported. If the non-user clicked the first option listed under **Report a Violation** – ***Impostor Accounts*** – they were presented with three options and instructions for reporting followed by the statement *"Go to the profile (timeline)"*.

We noted that within one of the options '*How do I report something on Facebook I can't see'* it was in fact possible for a non-user to make a report

> *"If you're blocked from reporting something that violates our Community Standards please* ***file a report here****"*

If the non-user clicked – "*please* ***file a report here****"* they were taken through to the appropriate screen to make a report but this Office considered the route to this point was unclear

FB-I in response has enhanced the means available to non-users wishing to report abuse. Now if a non-user clicks on 'Help' from the homepage of facebook.com they will be taken to a screen which contains a link to **'How to Report Abuse'** and if this is clicked they are presented with a range of options on the following screen, the last of which is **'Something You Can't See'** which would apply to all non-users if the content generating concern is posted on a non-public Facebook page. If the non-user clicks **'Something You Can't See'** they are taken to a screen which clearly states

> "If you're unable to use a report link because you don't have a Facebook account or you can't see whatever you're trying to report please file a report here."

The user is then taken to the appropriate page where they can report the abuse. We are satisfied with the steps taken by FB-I in this regard. This is obviously an area however that must be kept under continuous review to ensure that users and non-users alike are able to bring issues immediately to the attention of Facebook for action if that is appropriate.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION
Abuse Reporting	We are satisfied that FB-I has appropriate and accessible means in place for users and non-users to report abuse on the site. We are also satisfied from our examination of the User Operations area that FB-I is committed to ensuring it meets its obligations in this respect.

2.17 Compliance Management/Governance

As FB-I is designated as the responsible entity for all users of Facebook outside of North America, a crucial issue for this Office in our December Audit was to assess the substance of the control and influence of FB-I over the processing of data involved. We wished to establish that FB-I was in a position to be fully accountable for all uses of personal data by it. In overview terms, we expressed satisfaction with the structures and resources in place to meet these responsibilities but did articulate a concern "that products and features developed by engineers predominantly based in California and subjected to privacy reviews by legal teams outside Ireland will not be capable of fully understanding and complying with Irish and EU data protection requirements." In response we made the following recommendation in response to which FB-I made the commitment outlined.

Recommendation: This Office requires that Irish data protection law and by extension European data protection laws be fully addressed when FB-I rolls-out a new product to its users. We recommend therefore that FB-I take additional measures in the first half of 2012 to put in place a more comprehensive mechanism, resourced as appropriate, for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law.

FB-I Commitment: FB-I already fully considers and analyzes applicable laws, including Irish and EU laws, prior to product rollouts, but will implement this recommendation and consult with this Office during the process of improving and enhancing its existing mechanisms for ensuring that the introduction of new products or new uses of user data take full account of Irish data protection law.

Progress on this recommendation was a bottom-line issue for this Office throughout the year in our contacts with FB-I. The responsibility held by FB-I for all users outside of North America is immense. As we have made clear it is not a responsibility that can be met by the allocation of resources in Facebook Inc. It is for FB-I under Irish data protection law to ensure that it meets its heavy responsibilities for the personal data it processes. Our December Audit highlighted that FB-I on a day to day basis through its user operations and policy casework teams was meeting its responsibilities for user data but that we retained concerns about how it was resourced to meet its responsibility to be accountable for personal data for which it was responsible.

This was understood by FB-I and it has responded in terms which this Office considers are acceptable and will place FB-I in a better position to meet its data protection responsibilities in the EU. These developments are detailed in the FB-I Update Report as follows and elaborated upon in Appendix 1 of that Report:

"FB-I has appointed a senior lawyer as Head of Data Protection in Dublin, who has formed a data protection compliance team with members from legal, policy, platform, law enforcement, security, engineering, and user operations in Dublin, as well as ad hoc members located elsewhere in the EU, and the United States. The team's focus will be on ensuring data protection compliance in all areas of the operation of Facebook. The team will work closely with counterparts in entities responsible for processing user data. See Appendix 1 – Data Protection Compliance Team.

The FB-I data protection compliance team will work closely with counterpart teams in Facebook, Inc. Specifically, the Head of Data Protection will be involved in all product review prior to the launch of products in the EU, and will be responsible for ensuring that products and features comply with Irish data protection law prior to launch in the EU. Facebook, Inc. has established a product review structure that is led by its two Chief Privacy Officers (one for Product and the other for Policy). The Head of Data Protection will be part of the product review team."

This Office welcomes this commitment to meeting its data protection responsibilities by FB-I. The need to have this compliance team in place and making a strong contribution to product development and launch was demonstrated in the weeks prior to our onsite visit from 10-13 July by the temporary launch of the "Find Your Friends Nearby" feature by Facebook. As the feature was only live on Facebook for a matter of hours this Office has not assessed whether it complied with data protection requirements, rather our focus was to assess whether there were any lessons to be learnt from the launch.

Our particular focus was to examine from an engineering perspective what the process was for submitting updates to the live Facebook site. As a constantly evolving technology platform, there is a constant process of bug fixing, text updates, user testing and substantial feature updates taking place. Responsibility is placed on individual engineers to ensure that prior to submitting an update for the site that they have followed procedures. Straightforward matters such as bug fixes are still subjected to a peer review process whereby another engineer must sign off on the change prior to it being accepted for update for the site. This process was also followed in relation to the launch of the "Find Your Friends Nearby" feature. The issue that arose was that the engineer responsible for the feature had understood that the feature was progressed in line with the requirements set out in the procedures within Facebook for the examination of new features and products as previous discussions had taken place on the issue.

In the experience of this Office, Facebook in line with most technology companies is a heavily engineering oriented environment. There is, of course, nothing wrong with this as it is the genesis of the innovation which has made Facebook so successful. However, this engineering focus also creates risk that privacy and data protection issues may not always feature as high

as a priority at product planning and development stage as this Office may wish to see. In order to deal with this issue Facebook has outlined the procedures in place in the US and the input from FB-I to that process now to this Office.

Nevertheless in the view of this Office certain procedures in the product/legal review were not followed in the above manner on this occasion and this Office therefore sought clarity from FB-I as to the steps which it had taken on foot of this issue arising to mitigate the potential for a recurrence. In response it indicated that the product engineer had taken various earlier versions of the product through product/legal review and, when ready to launch, believed that the product had been fully vetted. In the meantime, Facebook established the above product review process, which, it has indicated had it been in place when the product engineer was in the earlier phases of development, the product would have gone through. FB-I has provided an assurance that the feature will be reviewed according to its new process prior to any future launch.

On a more general basis while this Office notes the steps that Facebook Inc has in place to review products and features prior to launch and while we also note that these incorporate input from FB-I, the compliance responsibility for meeting data protection requirements rests with FB-I. Therefore this Office expects all significant changes to the use of personal data with a data protection impact to be approved by FB-I in a manner set out by the Board of FB-I that takes full account of European data protection requirements.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Compliance Management/ Governance	We found that the compliance requirements for the conduct of direct marketing by electronic communications means had not been fully understood by certain FB-I staff members engaged in marketing. We recommend that documented procedures be developed to ensure that data protection considerations are taken fully into account when direct marketing is undertaken either by or on behalf of FB-I and that appropriate training be given to staff and contractors.	Complete at the time of publication of the December Audit
	This Office requires that Irish data protection law and by extension European data protection laws be fully addressed when FB-I rolls-out a new product to its users. We recommend therefore that FB-I take additional measures in the first half of 2012 to put in place a more comprehensive mechanism, resourced as appropriate, for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law.	Ongoing. All significant changes to the use of personal data with a data protection impact to be approved by FB-I in a manner set out by the Board of FB-I that takes full account of European data protection requirements.

FINAL REPORT

REPORT ON FACEBOOK IRELAND (FB-I) AUDIT 2-3 May & 10-13 JULY 2012

21st September 2012 / Prepared for the Data Protection Commissioner by FTR Solutions

Dave O'Reilly,
Chief Technologist,
FTR Solutions
E: **dave.oreilly@ftrsolutions.com**

Introduction

This document contains the results of the technical analysis conducted during the audit of Facebook carried out between the 2nd and 3rd May and between the 10th and 13th July 2012. The purpose of this audit was to examine a range of issues identified by the Office of the Data Protection Commissioner. A staff member from the Office of the Data Protection Commissioner assisted with the on-site testing and analysis.

In line with the methodology used in the original technical analysis, wherever possible sources of evidence have been sought and experiments carried out to validate that features described in this report perform as described. Every effort has again been made to make the test results produced in this report as repeatable as possible.

There are two main aspects to the technical analysis reported here;

- To obtain assurance that the findings of the technical analysis carried out as part of the audit in December 2011 continue to accurately reflect reality. A series of tests to validate these findings have been carried out. The results of this phase of the testing can be found in part one of the report below.
- An examination of functionality that was not studied as part of the first technical analysis has also been performed, details of which can be found in part two of this report.

Testing Environment

Unless otherwise described, all tests were performed in a newly installed, fully patched Windows XP virtual machine with antivirus software installed and updated. All browsing was carried out using the default configuration of Internet Explorer 8. A snapshot of the virtual machine state was taken and the snapshot was restored before each test described in this document unless explicitly explained otherwise.

Wireshark version 1.6.3 was used for all tests involving packet capture and analysis.

Facebook platform app development testing was performed by developing test applications with PHP5, using the Facebook PHP API version 3.1.1. The code of the Facebook PHP SDK was reviewed and the relevant aspects were confirmed to operate as reported.

Facebook mobile application testing was performed on the version 4.1.1 of the Facebook iPhone application and version 1.9.6 of the Facebook Android application. These were the most current versions at the time of testing.

The creation of the volume of Facebook accounts which were required to facilitate the testing described herein by the same computer/IP address was identified by Facebook's automated site integrity features as an unusual pattern of user behaviour. Consequently, after a certain point

attempts to create new Facebook accounts were blocked, requiring entry of a unique mobile phone number to verify the authenticity of the account. Accounts blocked in this way were manually unblocked by FB-I to facilitate the technical testing.

As with the original testing, and in order to verify certain claims, aspects of the Facebook source code have been examined. Source code examination took place by examining the contents of the FB-I source code repository. All examinations were carried out on the trunk of the repository, representing the currently deployed code base.

1 Part 1: Repeat Testing

1.1 Contact Importing

When a user creates a Facebook account, they have the opportunity to import contacts from a range of e-mail service providers to Facebook. It is possible that the user's contacts will include both users and non-users of Facebook. As well as sending friend requests to existing Facebook users, the user performing the contact import has the opportunity to invite the non-users to join Facebook and become friends.

If the user sends an invitation to a non-user, this will cause the non-user to receive an e-mail from Facebook containing a link that will allow the non-user to create a Facebook account.

The non-user can ignore this e-mail if they do not want to join Facebook. A link is provided in the invitation e-mail that allows the non-user to choose to opt out of receiving subsequent invitation requests from Facebook.

It is possible that a second Facebook user could import the same non-user e-mail address. Assuming that the non-user does not choose to opt out of receiving invitations, a second invitation could be sent to the non-user by the second Facebook user. The second (and subsequent) invitations may include reference to other Facebook users that the non-user may know.

1.1.1 Storage and Removal of Contact Data

As part of the previous audit, a review was performed of the data structures within which imported contact information is stored. These data structures were re-examined as part of this audit.

While the structures themselves have not changed in the period since the initial audit, an increased understanding of the structures gained in this audit has enabled greater clarity of how imported contacts are stored.

The imported contact information appears to be stored in the following way(s):

- Each time a user performs an import, the imported data is added to an array of imports, one entry for each set of imported data. Each entry in this array consists of a data structure containing an array of the contact names and a corresponding array of the contact e-mail addresses. This information is associated with the importing user's Facebook account.

- A data structure consisting of a hash of the e-mail address of the imported contact and the string consisting of a comma separated list of Facebook user IDs for users that have imported that particular e-mail address.
- A data structure containing a list of non-users to which the user has sent invitations.

In the initial technical report, it was stated that two other data structures referred to as "the user's address book" and "the user's phone book" were also populated with non-user contact information. Upon re-review it has been confirmed that in fact the address book and phone book are both generated from the array of imported data mentioned above.

Once again, no other storage of contact information about non-Facebook users has been identified.

The source code invoked when the user requests deletion of all imported contact data[1] has been re-reviewed. It has been confirmed that the following steps are carried out:

- All data is removed from the array of imports.
- The Facebook user ID of the user requesting the removal of the imported data is removed from the comma separated list of user IDs associated with all of their contact e-mail addresses. If there are no remaining user IDs associated with a particular contact e-mail address, the contact e-mail address entry is also removed. This continues to imply, as mentioned in the first report, that if a single Facebook user imports a particular contact e-mail address and that user subsequently removes their imported contacts, then all reference to the imported contact will be removed from this structure.
- The fact that the user has sent invitations to particular non-users is not deleted if the user requests deletion of all imported contact data because these are valid outstanding friend requests. It is, however, possible for the user to select and remove invites using the invite history page[2].

1.1.2 Use of Contact Data

As described in the first report, and verified in the second audit, there are only a small number of tasks that a user can perform with the imported contact information. In particular:

- The user can send invitations to the important contacts to become friends
- The user can remove the imported data

As part of the first audit, how the imported contact data is used by FB-I to make "People You May Know" suggestions was considered. At that time, detailed technical documentation for the "People You May Know" functionality was provided by FB-I and reviewed. FB-I have confirmed

[1] Invoked when the user selects "remove all your imported contacts" from the "Manage Invites and Imported Contacts" page.
[2] http://www.facebook.com/invite_history.php

that the use of the imported contact data to generate "People You May Know" suggestions has not changed since that time.

For completeness, the findings of the initial report in relation to the use of imported contact data to generate people you may know suggestions are included again here. Recall, the imported contact data may consist of both existing Facebook users and non-users. Considering these cases separately:

- It was noted in the case of existing Facebook users in the imported contact data:
  - That the existing Facebook users may be used as the basis of "People You May Know" suggestions
  - Other Facebook users who have imported the existing Facebook user as a contact may also, in some circumstances, be used as the basis of "People You May Know" suggestions.
- It was noted in the case of non-Facebook users in the imported contact data:
  - That two Facebook users that have only a non-Facebook user imported contact in common does not appear to cause the two users to be suggested to each other as "People You May Know". This is consistent with the documentation provided by FB-I detailing the operation of the "People You May Know" functionality.
  - If multiple Facebook users have imported the same non-user e-mail address, invitations sent to the non-user may contain suggestions of other users that have also imported the non-user's e-mail address. Users who have already sent invitations to the non-user do not appear to be suggested in subsequent invitations.

Based on both the first and second audits, the evidence would seem to indicate that the functionality by which Facebook users are suggested to each other as possible friends (referred to above as "People You May Know") and the functionality by which users are suggested to non-users in invitations operate on separate principles. FB-I have also re-confirmed that these two pieces of functionality are separate.

1.1.3 Non-user Opt Out

When a non-Facebook user chooses to opt out of receiving subsequent invitations from Facebook, a hash of their e-mail address is created and stored. A hash is a one-way function that generates a unique value representing a particular e-mail address[3].

[3] As mentioned in the initial report, there is a remote possibility of two email addresses having the same hash value. This is known as a hash collision. In the case of non-user opt out, a hash collision would lead to a scenario where a non-Facebook user who had not opted out of receiving emails would not receive emails from Facebook because the hash of their email address matches the hash of the email address of another non-Facebook user who has opted out of receiving emails. In particular, this would not lead to a situation where Facebook could recover non-user email addresses from stored hash values.

Scenarios can arise where Facebook user activity could cause the non-user to receive e-mail invitations. An example would be if a second user attempts to invite the non-user to join Facebook. The fact that the non-user's e-mail address matches a hash in the list of opted out e-mail hash values will prevent the e-mail from being sent.

In the first report, FB-I provided a list of all the possible ways that a non-user of Facebook could receive an e-mail from Facebook. The list provided at the time was:

- A user invites a non-user to join Facebook
- A user sends a private message to a non-user
- A user creates an event and invites a non-user to the event

At the time of writing of this report, it is no longer possible for a user to invite a non-user to an event.

Therefore, the impact of the user having opted out is that they will not receive any more invitations to join Facebook. This functionality has been retested and confirmed to work as described.

An opted out non-user will still receive private messages sent by users of Facebook from within Facebook similar to the way that any email service operates.

1.1.4 Import Password

When importing contacts from an e-mail account, the user can provide Facebook with the username and password of the supported e-mail provider. Facebook will then use these credentials to connect to the e-mail provider and import contacts.

The code used to perform this functionality has been re-examined and it has been confirmed, as it had been in the first audit, that the e-mail provider password is stored in memory for the duration of the import task and then discarded.

1.2 Synchronising

Facebook provide a mobile platform for allowing users to interact with Facebook on their mobile devices[4]. In the previous report, testing was performed on the contact synchronisation feature of the mobile application. The contact synchronisation functionality of the mobile application allows users of the application to synchronise the contacts in their address book with their Facebook friends.

[4] http://www.facebook.com/mobile/

1.2.1 Transmission of Contact Information

As part of the original report the data transmitted by the iPhone Facebook application was captured while contact synchronisation was taking place. This information was examined and it was noted at the time of the original report that the user's contact data was transmitted in plain text.

As part of this review, this testing has been repeated on both the iPhone and Android Facebook applications. It has been confirmed that in both cases the data transmitted while contact synchronisation is taking place is now encrypted.

1.2.2 Contact Synchronisation vs. Find Friends

As discussed in the first report, the Facebook iPhone[5] and Android[6] applications have two closely related features, contact synchronisation and find friends. The purpose of the contact synchronisation functionality is to provide Facebook users with a way to back up their contacts from their phone. The purpose of the find friends feature is to provide Facebook users with a way to search through the contacts on their phone for other Facebook users to become friends with and to invite non-Facebook users in their contacts to join Facebook.

The first report made several observations about these two features. These were:

- After contact synchronisation was enabled, the contact information is not accessible from the user's "Manage Invites and Imported Contacts" page.
- Contact synchronisation can be disabled at any time through the mobile application.
- The act of disabling contact synchronisation does not delete any of the synchronised data.
- There is a "Remove Data" button in the mobile applications that removes data transferred from Facebook to the mobile device. This information will have been added to the address book on the mobile device and can include profile photos, birthdays and Facebook URLs.
- To remove the data transferred to Facebook from the mobile device requires the user to visit "Manage Invites and Imported Contacts" on the Facebook website and click "remove all your imported contacts", even though the contact information is not visible in "Manage Invites and Imported Contacts".
- Using Facebook internal tools it was confirmed that when "remove all your imported contacts" is selected that all synchronised contact information has been deleted. This is

[5] The testing in the original report was performed on version 4.0.2 of the Facebook iPhone app. The testing for this report was performed on version 4.1.1 of the Facebook iPhone app, which was the latest version of the app at the time that the testing was performed. In the time between the testing and the completion of the report, version 5 of the Facebook iPhone app has been released and announcements have been made of integration of Facebook functionality into iOS 6. Neither version 5 of the Facebook iPhone app nor Facebook integration into iOS 6 has been examined as part of this work.

[6] The Android application was not reviewed as part of the first report.

the same process followed when contacts are imported from any source as described in Section 1.1 with the proviso that removed contacts will be re-imported automatically unless you turn off contact synchronisation in the mobile application.

- When the find friends button is clicked, the user's address book information is presented in two categories; contacts that are existing Facebook users and non-Facebook users. The user can choose to send friend requests to existing Facebook users and invitations to non-Facebook users. Both sets of users are presented with an option to simultaneously send friend requests or invitations to all contacts being presented.
- Only after the find friends button has been clicked is the contact information visible in the "Manage Invites and Imported Contacts" Facebook page.

The testing carried out as part of the first audit has been repeated and the findings described above continue to be an accurate reflection of the operation of the functionality at the time of testing. The imported contact deletion code was also re-reviewed to confirm this.

As mentioned in the footnote of Section 1.2.2, a new version of the iPhone application, version 5, has been released in the meantime. Testing has not been performed on this version, but FB-I report that the contact synchronisation feature has been removed from this version.

The repeat testing has identified the following additional point which must be clarified; If the user has chosen to send friend requests to Facebook users or invitations to any non-users from their imported contacts, the fact that these invitations have been sent is not deleted when the user clicks "remove all your imported contacts" because, as discussed in Section 1.1.1, these are valid outstanding friend requests.

1.2.3 Use of Non-Facebook Synchronised Contacts, Imported Contacts and Invites in "People You May Know" Calculations

In the first audit, a series of tests were performed to understand how synchronised contacts, imported contacts and sent invitations related to the generation of "People You May Know" suggestions. The results were as follows:

- Any existing Facebook users in synchronised contacts will be suggested as people you may know.
- The fact that two Facebook users have a non-Facebook user contact in common does not appear to change the "People You May Know" suggestions for either user. In particular, the two users who only have the non-Facebook user contact in common are not suggested to each other as "People You May Know". This appears to also be true if both of the Facebook users have sent invitations to the non-Facebook user (which the non-Facebook user has ignored).

The testing has been re-performed and the findings above have been found to continue to accurately reflect the behaviour of the site.

As part of the first audit FB-I provided detailed technical documentation for the “People You May Know” functionality. The documentation indicated that non-user data is not used to generate “People You May Know” suggestions. FB-I have confirmed as part of this audit that the use of contacts and invites in “People You May Know” has not substantially changed in the intervening period. The results of the testing described here, and in the first audit report, continue to be consistent with the documented functionality.

1.3 Data Security

As per section 4 of the original technical report, data security has been divided into two sections; security of user communication with Facebook and Facebook corporate information security.

1.3.1 Security of User Accounts

Briefly summarising the findings of the original technical report;

- FB-I provide a range of base security features by default on all accounts. The most obvious of these are the credentials used to login. However, FB-I also monitor for suspicious activity on user accounts. Detection of suspicious activity will lead to additional authentication steps such as the user needing to fill out a CAPTCHA or by an SMS authorisation code sent to the user's mobile phone.
- Facebook also provides a selection of opt-in security features accessible via the user's account settings. These are;
    - Secure browsing: enables the use of encrypted communication using HTTPS wherever possible.
    - Login notifications: involves notifying the user whenever their account is accessed from a computer or mobile device does not been used before.
    - Login approvals: involves entering the security code, sent to the user by SMS, each time the user's account is accessed from a computer or mobile device that has not been used before.
    - Active sessions: allows a logged in user to see the locations from which their account is currently logged in and end activity from any particular session if that activity is unrecognised.
    - One-time passwords: allows users to protect their account when the login from a public computer. The user sends an SMS to a particular number and they will receive an eight character temporary password, valid for 20 minutes, which can be used to access their account. The availability of the one-time passwords feature appears to depend on country and mobile operator.
- Facebook maintains a security centre to provide a resource to educate users about staying safe online maintaining the security of their account.

It has been verified that these features continue to exist and continue to operate substantially as described in the original technical report.

The original technical report stated that secure browsing was not supported on the mobile platform. It has been confirmed as part of the current testing that communication is encrypted using TLS[7] (version 1.2) between Facebook and both the iPhone and Android Facebook applications. TLS version 1.2 is an industry standard encryption algorithm and is believed to offer adequate security.

1.3.2 Corporate Information Security

In the previous audit an attempt was made to gain an overall understanding of information security controls in place within FB-I. At that time it was further concluded that the majority of the controls described by FB-I appeared to be operating effectively. Information security controls within FB-I have not substantially changed in the intervening months and it is therefore concluded that FB-I continue to maintain and adequate information security stance.

It was noted at the time of the previous audit that FB-I expend considerable effort to manage employee access to user data. This second review has been used as an opportunity to study this matter in considerable detail. The results of this examination can be found in the following sections.

Access to user data is controlled by permissions assigned through an internal permission management system. This permission management system uses a variation on a standard “user, role, permission” logical access control model. Access permissions are divided into broad categories known as domains. To a first approximation, domains can be thought of as roughly equivalent to individual internal tools[8]. Within a domain is a set of actions that can be carried out within the context of that domain. These actions are analogous to permissions[9]. The ability to perform any particular action can be assigned to an individual employee more commonly to a role. Employees can be assigned to these roles, which contain sets of permissions appropriate to a function within the organisation.

1.3.2.1 Account Provisioning

Employee accounts are automatically provisioned and de-provisioned based on updates to the employee’s entry in the human resource management system. The human resource system feeds information to an internal identity management system that is used to create accounts in an organisational database.

1.3.2.2 Granting Permissions

Permissions can be granted to employees in several ways:

[7] http://tools.ietf.org/html/rfc5246

[8] In some cases, two tools are so similar that they will have been aggregated into a single domain but the mapping between tools and domains remains a good first approximation.

[9] The terms “permissions” and “actions” are used interchangeably below.

- Roles can be configured to match patterns of employee information within the organisational database. An employee that matches such a pattern will therefore be automatically granted this role. These roles are defined in terms of parameters such as the employee's geographical location or job title. It is notable that if the employee's role changes in the human resource management system, this will automatically propagate to the organisational database and their account will therefore automatically be removed from any roles that are no longer relevant to their new position. No administrative action is required in these cases.
- An employee can also be manually added to a role or granted a specific action by an administrator based on an ad-hoc request. These requests are circulated by email to a per-domain list of approvers, which consist of the owners of the domain and also information security staff.
- Software engineers can self-grant themselves temporary access to a certain domain. This is predominantly used for bug fixing. A notification email is sent to the domain administrators when such temporary access has been granted and the permissions are automatically revoked after 14 days. This self-granting of permissions is only possible by software engineers.

A sample of automatic security roles was reviewed and it was confirmed that employees in these roles have the expected permissions. Membership of the sample roles examined was based on both the employee's geographic location and job title.

The workflow for an employee to request (and subsequently be granted) access to a domain was studied. When an employee who does not have permission to access a particular tool or to perform a particular function within the tool attempts to use functionality that they do not have access to, the employee is presented with a dialog box through which they can request access. The employee must provide a business justification for requiring access to the functionality along with their request.

The request is forwarded by email to the appropriate list of domain owners and information security staff. Any one of the members of the approval list can grant the requested access. The access can be granted either permanently or temporarily for 14 days. FB-I have provided a copy of documented guidelines for tool administrators to assist them in determining whether or not requested permissions should be granted. These guidelines have been reviewed and it has been concluded that the guidelines provide adequate information to a tool administrator to enable them to make a sensible decision as to whether to approve or deny an incoming permission request.

When the access has been granted, an email notification is sent back to the employee who requested the access and is also copied to the entire list of approvers. This mechanism allows oversight of the actions of each individual approver by the entire list of approvers.

The list of access requests for a sample 30 day period were reviewed to determine what proportion of requests are approved by the domain owners and what proportion are approved by

information security. In the period examined, 46.54% of the access requests received were approved by information security.

One of the advantages of the model adopted by FB-I for granting permissions to domains is that the domain owners understand in detail the operation of the tool and are therefore well placed to determine whether access requests by employees are appropriate. The large percentage of requests approved by the information security team appears at odds with this justification. However, the transparent nature of the approval process means that the domain owners continue to have oversight of permissions granted even if they did not approve the request themselves. It was reported by FB-I that this number of requests in the sample period is atypically large due to an artifact of the ongoing migration from statically configured roles to the automatically assigned roles described earlier. FB-I reports that a more representative number of permission requests would be in the region of 30 per week.

Software engineers can self-grant temporary permission to access any tool. The workflow by which software engineers go about gaining permissions has been examined in detail and is summarised here:

- Typically in response to a report of a bug, an engineer visits a tool and attempts to perform an action for which they do not have permission.
- The engineer receives a permission denied screen that contains a “Get Permission Now” button.
- When the “Get Permission Now” button is clicked, the engineer fills in the reason why they need the access.
- On the same screen, prior to submitting the request for the permission, the engineer is warned to be careful and a reference to the acceptable usage policy is included on the screen[10].
- The engineer is then granted permission to access the tool for two weeks.
- When engineers grant themselves permission to a tool in this way, an email is received by the domain owners stating that the engineers have granted themselves permission to the tool. This email contains the reason provided by the engineer as to why they needed access and also contains a link to FB-I’s internal CERT (Computer Emergency Response Team) where the domain owner can report inappropriate access by an engineer. FB-I report that such administrative reports are rare.

1.3.2.3 Revocation of Permissions

Permissions that have been granted using the techniques described in Section 1.3.2.2 can be revoked both automatically and manually.

[10] The wording of the warning is “Please be careful when interacting with internal tools, especially those that access user data. If you have any questions about whether you should proceed, please contact one of the admins listed above, email <INTERNAL SECURITY EMAIL ADDRESS REMOVED>, or consult the Acceptable Use Wiki Page.”

If the employee is removed from the human resource management system, this change will be automatically propagated to the internal organisational database and all user access will be revoked. If the employee's role is changed in the human resource management system such that certain roles that were automatically assigned based on job title are no longer applicable, the employee will be automatically removed from these roles.

An employee can be manually removed from a role, or have an action manually revoked by the domain owner or an administrator.

Non-role based permissions are automatically removed from employees if they are not used within 45 days. Temporary access, both self-granted and granted by an administrator, expires after 14 days.

Summarising the management of permissions in the cases of movers and leavers;

- If an employee moves role;
    - Permissions automatically granted based on the employee's old role will be automatically revoked.
    - Any unused permissions will be automatically revoked after 45 days.
    - The employee is sent an email and asked to confirm if they still need any remaining roles or permissions.
- If an employee leaves the organisation, all of their permissions are automatically revoked upon removal of their record from the human resource management system.

1.3.2.4 Logging of Permission Usage Activity

Extensive logging is carried out of activity surrounding permissions to access Facebook user data.

All successful and failed attempts to use any permission are logged. All administrative actions are logged including; adding or removing employees to/from a role, granting or revoking an action and generating an access token (see Section 1.3.2.5 for a description of the token-based access model).

These logs are actively analysed by the abuse detection mechanisms, described in Section 1.3.2.7, to detect inappropriate use of permissions.

1.3.2.5 Token-based Access Model

FB-I are in the process of adding a tokenised access model on top of the domain-based access model described above. Whereas the domain-based access model only allows permission to be granted at the level of granularity of an action within a domain the tokenised access model allows permissions to be granted at the level of granularity of an action for specific Facebook user within a domain.

FB-I employees access user data via tools in two different workflows:

- Inbound workflows are initiated by users, typically requesting support. This includes the tools used by FB-I user operations to track user support tickets.
- Proactive workflows are initiated by FB-I employees who discover an account through other means. For example, when a member of the site integrity team is investigating abuse.

Tokens are generated by inbound workflow tools as well as, at the time of writing, one proactive tool. Tokens can be generated to allow access to

- A single user ID
- A single user ID plus their friends
- Any Facebook employee

The tokens generated by the inbound workflow tools can then be used in other internal tools to resolve the users issue.

To consider a concrete example for clarity, FB-I user operations have access to a User Admin tool. This tool allows the user operations team member to view administrative data about a Facebook user's account, including their name, account status, registration date and recent account changes. In the domain based permissions model it was only possible to grant permissions to employees to use the tool. In other words, if an employee had the ability to use this tool it would be possible for the employee to view any user. With the token-based access model, an employee subject to the tokenised access model needs both permission to use the tool generally as well as a token for the specific user they want to view.

Migration to the token-based access model is well progressed. FB-I report, at the time of writing, that tokenised access is enabled for all inbound requests serviced by all teams within FB-I.

Not all support tasks are initiated by an inbound service request from the user. These "proactive" workflows present a greater challenge for the token-based access model. FB-I have an ongoing project to identify individual proactive workflows that are candidates for tokenisation. In each case, FB-I intend to identify appropriate tokens to replace the current access model or else remove the need for employees to seek ad-hoc access to data by reworking processes. FB-I report that it is difficult to estimate timeframes over which these processes will migrate to the token-based access model since many of the changes to the proactive workflows have engineering implications that are not fully understood in advance. A risk-based approach is being used to examine the proactive workflows and prioritise the migration to the token-based model. Even though these proactive workflows are not tokenised, they are still logged and audited to provide oversight and abuse detection, as described in Section 1.3.2.7 below.

1.3.2.6 Administrative Privileges

It is possible for an administrator of a domain to create other administrators for that domain using the permission manager tool. Notification of the granting of the administrator access will be emailed to all of the administrators of that domain, just as with the granting of any permission, so it is possible for one of the other administrators to escalate the issue if the granting of the administrative access is not appropriate. FB-I provided a copy of guidance provided to tool administrators to assist them in determining whether a request for administrative privileges should be approved. These guidelines have been reviewed and it has been concluded that the guidelines provide adequate information to a tool administrator to enable them to make a sensible decision as to whether to approve or deny an incoming permission request.

During the audit, testing was been carried out to determine whether it is possible for a software engineer to self-grant themselves administrative privileges to a domain. The testing was performed by FB-I under observation. Two different techniques were attempted.

Firstly, an attempt was made to grant privileged access by browsing to a tool where access is denied and clicking “Get Permissions Now”, as described above. Administrative access is not accessible via this route.

Secondly, by visiting the permissions manager tool and browsing to the target domain an attempt was made to add oneself as an administrator of the domain. This fails with the message “Permission denied: you must be an admin of the given domain to perform the requested action. If you need administrative privileges for this domain, please contact one of the existing admins.”

The permission manager activity logs were reviewed and it was confirmed that the failed attempts to grant the administrator privilege were logged. These logs are actively analysed by the abuse detection mechanisms, described in Section 1.3.2.7, to detect inappropriate use of permissions.

1.3.2.7 Abuse Detection

FB-I leverage logs from various sources, including the permission usage and administration logs, to proactively search for employee abuse of access to user data.

Two separate tools have been demonstrated by FB-I and described in detail.

The first tool focuses specifically on analysis of the permission usage and administration logs. The tool examines all permission usage and seeks patterns that would indicate abuse. Some examples of suspicious patterns are;

- Numerous failed attempts to use a particular permission, followed by successful use of that permission.
- A relationship between an employee and the data they are accessing. For example, an employee accessing their wife’s data.

- Access to sensitive user accounts (e.g. celebrities).
- Deviations from a normal usage pattern. For example, an employee accessing a disproportionate number of female user accounts when a typical access pattern for an individual in a similar role is 50% male, 50% female.
- Issuing refunds to a user with whom the employee has a relationship.

An email report is generated daily from this tool and sent to two independent security teams for review.

The second tool gathers logs from various sources throughout the organisation and detects anomalous activity by recognising when observed behaviour deviates from expected behaviour. The list of information gathered and analysed by this tool has been reviewed and confirmed to contain a wide range of privileged activities. Expected behaviour is defined in terms of the employee's normal usage pattern, the usage pattern of other employees in the same department and the usage pattern of all employees in the organisation.

These reports are also generated once per week and are sent to the two independent security teams for review.

Evidence of the delivery of automated email reports to security teams has been provided.

If a security team member, while examining one of the reports, believes that an abuse incident has taken place, they escalate the matter to HR and legal for further review and action. Facebook supply documented guidance to the security team to assist team in determining whether a particular incident constitutes abuse. The guidance documentation has been reviewed and confirmed to provide guidance consistent with the representative list of suspicious activities listed above.

Facebook have a further control in place to prevent employees covertly accessing other employee's accounts; If employee A accesses employee B in the user admin tool, employee B will receive an email notification stating that employee A has accessed their data. If this access is not authorised, employee B can raise an incident with the security team, which will be handled as described above. A legitimate use-case for employees accessing each other's accounts would be if a software engineer needed access to an employee's account to resolve a reported bug.

Finally, Facebook have also deployed a network intrusion detection system to detect anomalous behaviour that may indicate a data breach or attempted data breach.

1.3.2.8 Sample Permissions Review

A random sample of employees was selected and the permissions granted to those employees were reviewed to determine whether they were appropriate for the roles of the individuals within the organisation.

The permissions of the employees and the level of access to user data were consistent with, and not excessive for, the roles of the selected individuals.

1.4 Application Development

1.4.1 Background

Facebook provide an application platform to allow third party developers to build applications that integrate with the Facebook platform[11]. Facebook also provide platforms for integration with other websites (e.g. social plugins discussed in Section 0) and integration with mobile applications.

In the previous audit, testing was performed to explore the functionality provided by the Facebook web application platform. Web platform applications conform to the following basic architecture:

- Facebook applications are loaded into a canvas page that is populated by the third party application. An example URL of a canvas page would be https://apps.facebook.com/SimpleTestApplication/. This is the URL through which the user interacts with the application.
- The third party developer provides a URL, known as the canvas URL. Facebook submits requests to the canvas URL in order to retrieve content for presentation to the user on the canvas page.
- The content retrieved from the canvas URL is loaded within an iframe on the canvas page.
- Facebook submits information about the user of the third party application to the canvas URL in the form of a HTTP POST with a single parameter called signed_request. This parameter is a base64 encoded JSON object that must be decoded by the third party application before processing.

1.4.2 Application Access Control

Application access to user account information is controlled by permissions. The application must request permission to gain access to various types of information or perform actions on the user's account. The minimum amount of access that a user can provide an application will allow that application to access their basic information. The basic information is:

- User ID
- Name
- Profile picture
- Gender
- Age range

[11] http://developers.facebook.com/

- Locale
- Networks
- List of friends
- Any other information the user has made public

Access to other information about the user or their friends requires that the application request extra permissions from the user. After having authorised an application, the user can revoke the authorised permissions through their account settings.

Certain types of permissions are required by the application and can only be revoked by de-authorising the application entirely. Other permissions can be revoked individually.

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.

1.4.3 Before Authorisation

Before a user authorises an application to access any of their information, it has been confirmed that the application is able to access the country, locale and age range of the user. These parameters are provided so that an application developer can ensure that the content delivered by the application is appropriate for the age and country of the user and is also localised appropriately.

In the previous audit, the content of the HTTP request headers received by the canvas URL from Facebook were examined to ensure that the HTTP headers do not contain any user identifying information. In particular, it was verified that the HTTP referrer header does not contain the user ID of the browsing user. This fact has been reconfirmed as part of this audit.

1.4.4 Application Authorisation

When the user has authorised an application to access their account according to a particular set of permissions, the application is provided with an authorisation token. The token is then provided to Facebook along with subsequent requests for information. All testing in both this audit and the first audit was performed using the server side authentication flow[12].

It has been re-confirmed that only basic information, as described above, 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. In particular:

- If the application has not been granted the "user_photos" permission, a request to view the content of a user album that is shared only with friends fails.

[12] http://developers.facebook.com/docs/authentication/

- If the application has been granted the "user_photos" permission, a request to view the content of a user album that is shared only with friends succeeds.
- If the application has not been granted the "publish_stream"[13] permission, an attempt to post a message to the user's wall fails.
- If the application has been granted the "publish_stream" permission, an attempt to post a message to the user's wall succeeds.

1.4.5 Access to User Friend Information

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

- 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 therefore have access to User B's photos

Unless the friend has opted out as described below, the same basic information listed in Section 1.4.2 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. These configuration settings are available in Privacy Settings->Ads, Apps and Websites[14] in the section entitled "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 re-confirmed that if, in the above example, User B had unchecked "My Photos" in their privacy configuration, an application installed by User A can no longer see User B's photos. Note that User A will still be able to interactively view User B's photos by browsing to User B's profile for example, but applications installed by User A will not.

If a user does not want any information, or even their existence shared with applications that their friends install, they must disable the application platform. This can be achieved by selecting "Turn off your ability to use apps, plugins, and websites on and off Facebook" in Privacy

[13] In the time since the first audit, the "publish_stream" permission has updated their documentation to recommend that applications implement a user-initiated sharing model rather than using the "publish_stream" permission to post content to the user's news feed without their explicit knowledge and consent.
[14] The arrangement of the privacy settings has changed since the first audit. The location of this configuration used to be called Privacy Settings->Apps and Websites.

Settings->Ads, Apps and Websites[15]. It has been re-confirmed that if a user decides to do this, not even their basic information is visible to applications that their friends install. However, when the application platform is disabled the user will not be able to use any applications themselves.

1.4.6 Duration of Validity of Token

At the time of the first audit, it was noted that the default validity period of tokens generated by authorisation requests was 2 hours. It has been re-confirmed that the default validity of tokens generated by authorisation requests is up to 2 hours[16].

In the first audit, the presence of the "offline_access" permission was noted. This permission allowed an application to perform actions on the user's behalf at any time. Tokens granted with the "offline_access" permission did not expire after any period of time. Rather, the token was invalidated on the occurrence of certain events such as the user changing their password or suspicious activity on the user's account.

In the time between the first audit and this audit, the "offline_access" permission has been deprecated and, at the time of writing, is scheduled for removal from the developer platform in October 2012[17], [18].

The "offline_access" permission is being replaced by an alternative mechanism where an application can exchange a default, short-lived token for a longer-lived token with a validity period of 60 days. The longer-lived token can then be re-validated by the application each time the user visits the application, emulating the behaviour of an "offline_access" token, as long as the user visits the application at least once every 60 days.

The advantage of the new system over the older one is that applications that a user is no longer engaging with will not have indefinite access to the user's information.

After the migration period to the new scheme, all tokens granted with the "offline_access" permission will have their validity period truncated to 60 days.

1.4.7 Transferability of Authorisation Token

In the first audit report it was noted that the validity of an authorisation token is not dependent on the source of the request and that the application secret is not required to generate valid authorisation tokens.

[15] At the time of the first audit, this setting was called "Turn off all platform apps" and was located in Privacy Settings->Apps and Websites.

[16] The online documentation states that the validity period is between one and two hours.

[17] https://developers.facebook.com/roadmap/offline-access-removal/

[18] https://developers.facebook.com/roadmap/

FB-I confirm that this is the expected behaviour of the permissions system, since a valid token grants the bearer of that token access to the corresponding information with the corresponding permissions. At the time of the first report, it was noted that the alternative to such as system is to require the application to generate a cryptographic signature, based on the application secret, for each submitted request.

FB-I provided two reasons for the selection of this architecture at the time of the first audit:

- The greater complexity of the code required to sign requests means that certain application developers were unwilling or unable to develop applications that use such a system. FB-I report that there is a strong correlation between the ease of use of an API and the uptake by the development community.
- Only a single use-case was considered as part of the audit, based on the server side authentication flow. Other use cases, such as the use of Facebook APIs in Adobe Flash applications or standalone executable files were not considered. In such cases, requiring the application developer to sign requests to Facebook often lead to the application secret being coded into the Adobe Flash or standalone application. It is then possible for a malicious individual to reverse engineer the application and retrieve the application secret. This security outcome is considered worse than the risk presented by the bearer token model.

Both of these points continue to be valid arguments for the bearer token model. This topic was re-visited as part of the second audit, and FB-I presented several additional arguments in favour of the bearer token model;

- An individual bearer token grants access to a specific user's information in a specific way to a specific application. The compromise of a bearer token has limited impact when compared to the impact of a compromise of an application secret key in the alternative model.
- It is not possible to rely on applications to correctly verify cryptographic signatures of responses sent by Facebook. In many cases the signature checking will simply not be carried out. Therefore, there is little point in incorporating a scheme of signing responses to applications.
- Even if there is intent and technical ability of an application developer to correctly use a cryptographic technique to either encrypt/decrypt or sign/verify communication between the application and Facebook, the fact that so many implementations of the same cryptographic algorithms work, or can be configured to work, in different and subtly incompatible ways makes this challenging. For example, differing shift-register widths or different padding algorithms used with the same cryptographic algorithm.
- Requiring application developers to provide a HTTPS canvas URL with which Facebook can interact now enforces the secure transport of application data.

On balance, therefore, it has been 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.

1.4.8 Reliance on Developer Adherence to Best Practice/Policy

In the first audit report, several scenarios were identified that required developer adherence to best practice or stated policy in order to ensure security of user data. These scenarios have been reviewed as part of the second audit to assess their status and note any changes.

1.4.8.1 Use of Secure Site to Host Application

When a user authorises an application, the authorisation token is submitted to the canvas URL provided by the developer when the application was set up.

As of 1st October 2011 Facebook require that authors of applications provide both a canvas URL and a secure canvas URL (i.e. a HTTPS URL). At the time of the first audit, around 3rd December 2011, it did not appear to be necessary to provide a secure canvas URL. It was possible to configure an application with only an insecure canvas URL and authorisation tokens were successfully delivered to this (unencrypted) URL.

This appeared to introduce a risk that unless the application developer provided a secure canvas URL, authorisation tokens could be intercepted in transit to the application.

This test was re-performed as part of this audit and it was confirmed that application developers are now required to provide a secure canvas URL for all new applications created. It has also been noted that if a previously created application did not have a secure canvas URL, changing the applications basic settings requires the application developer to provide a secure canvas URL.

1.4.8.2 Cross-Site Request Forgery (CSRF)

Cross-site request forgery is an attack where a legitimate user visits a malicious website which causes an action to be performed on the user's account without the user's knowledge.

The OAuth standard upon which the Facebook application authorisation framework is based allows the transmission of an opaque (to Facebook) state parameter that is returned to the caller along with the authorisation token. An application developer can use this feature to, amongst other things, ensure that the authorisation token is received in response to a known authorisation request. This technique reduces the risk of CSRF attacks.

At the time of the first audit, Facebook had strongly recommended in their application authentication documentation that any applications implementing Facebook user login implement CSRF protection using this mechanism. The documentation has been re-reviewed and it was noted that Facebook continue to recommend that this technique is used to reduce the risk of CSRF.

1.4.8.3 Storage of Access Token

In the first audit report it was noted that there was a risk associated with the theft of authorisation tokens from an application developer. This risk was noted as being particularly acute in cases where authorisation tokens with long periods of validity (i.e. “offline_access” tokens) had been granted. At the time it was further noted that the compromise in a third party developer of valid pairs of user ID and authorisation token would allow any application to gain equivalent access to the user account as the access granted to the original application for the period of validity of the authorisation token.

It is therefore necessary that application developers take appropriate steps to ensure the security of the authorisation tokens provided by Facebook.

It is notable that the functionality which replaces the “offline_access” token, described in Section 1.4.6 further mitigates against this risk, since no token has a validity greater than 60 days. In addition, when considered in the context of the alternative, the use of application secrets, the bearer token model is believed to provide an adequate balance between security and usability, as discussed in Section 1.4.7.

Further, Facebook has the ability to suspend an application’s access to the application platform, as well as to detect inappropriate actions and automatically disable suspicious application. In the case of stolen bearer tokens, the suspicious actions will appear to Facebook as if they are being performed by the legitimate application from which the authorisation token was granted by Facebook.

1.4.8.4 Increasing Access

Based on the permissions structure described in this section, an application that does not have access to a user’s private information cannot increase its access to that user’s information. In other words, a technical infrastructure prohibits unauthorised access to user data by applications.

However, it was noted at the time of the first audit that an application with access to some of a user’s private data could, hypothetically, increase the access that one user has to another user’s data beyond the access that would normally be allowed according to the user’s privacy settings. For example:

- User A only shares photos with friends
- User B is not a friend of User A
- User A authorises access to their photos to an application
- User B authorises access to their photos to an application
- The application has access to User A’s photos and were the application to present User A’s photos to User B for any reason, User B would have gained increased access to User A’s information.

Applications that increase access to information in this way are prohibited by policy. In was noted at the time of the first audit and confirmed at this audit that, *prima facia*, it appears extremely challenging to implement a technical solution to ensure that applications do not perform this type of action.

1.5 Social Plugins

1.5.1 Background

Social plugins are a feature provided by Facebook to website owners, allowing the owners of websites to provide a customised browsing experience to Facebook users. The social plugins allow users to see relevant information such as which of their friends have "liked" the content of the website.

When a logged-in Facebook user visits a website that has a Facebook social plugin, the user will be presented with personalised content based on what their friends have liked, commented or recommended upon the site.

1.5.2 Social Plugin Structure

Social plugin content is loaded in an inline frame, or iframe. An iframe allows a separate HTML document to be loaded while a page is being loaded. In this case, the social plugin content is loaded separately from the content of the surrounding website.

As part of the first audit it was confirmed that the content of the social plugin component of a web page is delivered directly to the web browser from Facebook, separately from the surrounding content from the website. This test has been re-performed as part of this audit substantially as described in the original report. Briefly the test performed was;

- A website containing a social plugin was visited. For testing, the website http://www.imdb.com/ was used.
- While the site was being loaded in the browser, all traffic generated was captured.
- The HTML source code of the social plugin was viewed.
- The DNS queries generated while the website was loading were examined and any IP addresses for www.facebook.com were extracted.
- The HTTP traffic to/from the Facebook IP address was examined and it was confirmed that the content of the HTTP response from Facebook is the same as the content of the social plugin iframe.

This confirms that the content of the social plugin iframe was delivered directly to the web browser from Facebook. Web browsers do not allow cross-frame communication or access to data served from different domains so it has therefore been re-confirmed that the site on which the social plugin is hosted does not have visibility of the content of the social plugin.

1.5.3 Non-Facebook Users and Cookies

During the first audit, several experiments were performed to determine what, if any, cookies were set and/or transmitted when a non-Facebook user visits websites with social plugins.

Two separate scenarios were identified as producing different results;

- A non-Facebook user who has never visited the Facebook web page
- A non-Facebook user who has visited the Facebook web page

To examine the case of a non-Facebook user who has never visited the Facebook page, a period of browsing was carried out in a test virtual machine. Care was taken not to visit the Facebook page. Some of the websites visited had social plugins and some did not.

All traffic was captured and all HTTP request/response pairs were individually examined. No Set-Cookie headers were received in any HTTP responses from Facebook. Cookies can be created in other ways, for example by JavaScript, but examination of the HTTP requests confirms that no cookies, howsoever created, are transmitted to Facebook in any HTTP request.

Therefore, it was concluded in the case of a non-Facebook user never having visited Facebook, no cookies are either sent to or by Facebook when a user visits websites containing social plugins.

This test was re-performed as part of this audit and it was confirmed that the behaviour was identical.

Considering the second case, a non-Facebook user who has visited the Facebook web page, a separate period of browsing was carried out in a virtual machine preceded by a visit to the Facebook web page. In the first audit it was noted that when a user visits the Facebook home page, three cookies were set;

- datr
    - This cookie was set with an expiry time of 2 years.
    - The path of the cookie was “/” and the domain was “.facebook.com”.
- reg_fb_gate
    - This cookie does not have an expiry time and is therefore a session cookie, which exists until the browser exits.
    - The path of the cookie was “/” and the domain was “.facebook.com”.
- reg_fb_ref
    - This cookie does not have an expiry time and is therefore a session cookie, which exists until the browser exits.
    - The path of the cookie was “/” and the domain was “.facebook.com”.

This was followed by a period of browsing to websites, some of which had social plugins and some of which did not. It was noted that the first HTTP request for social plugin content transmitted the cookies listed above along with a cookie named wd, presumably generated by JavaScript. The wd cookie had the value "1082x676" which represents the dimensions of the browser window in which the Facebook page was loaded. The HTTP response received from Facebook in response to this HTTP request unset the wd cookie.

The remaining cookies were transmitted in each of the remaining HTTP requests to Facebook for social plugin content.

This test has been re-performed as part of this audit and it was noted that when the Facebook page was visited at the start of the test, an additional session cookie named lsd was set. This cookie was also transmitted in each of the HTTP requests to Facebook for social plugin content.

As described in Section 1.5.5.12, the lsd cookie is used to prevent cross-site request forgery attacks.

1.5.4 Facebook Users and Cookies

Using a similar technique to the one described above, the cookies sent to Facebook user when a logged in or logged out Facebook user browses to sites containing social plugins were examined as part of the first audit.

1.5.4.1 Logged In Users

The Facebook website was visited and a user account was used to log in. A period of browsing activity to non-Facebook sites, some with social plugins and some without, then took place.

When the testing was performed as part of the first audit, it was noted that each request to Facebook for social plugin content transmitted the same set of cookies:

- datr
- c_user
- lu
- sct
- xs
- x-referer
- presence
- p

When the testing was repeated as part of this audit, it was noted that the following cookies were transmitted with each request for social plugin content:

- datr

- c_user
- fr
- lu
- xs
- x-referer
- presence
- p

Notably, there is an additional cookie, fr, which appears to be transmitted by Facebook. The purpose of this cookie, along with the others mentioned here, are described below in Section 1.5.5.

1.5.4.2 Logged Out Users

The Facebook website was visited again and a user account was logged in and immediately logged out. A period of browsing to non-Facebook sites, some with social plugins, some without, then took place. At the time of the first audit, it was noted that each request to Facebook for social plugin content transmitted the same set of cookies:

- datr
- lu
- x-referer
- locale
- lsd
- reg_fb_gate
- reg_fb_reg

When the testing was repeated as part of this audit, it was noted that the following cookies were transmitted with each request for social plugin content:

- datr
- fr
- lu
- x-referer
- locale
- lsd
- reg_fb_gate
- reg_fb_ref
- wd (sometimes)

Again it is notable that there is an additional cookie, fr, which appears to be transmitted by Facebook. The purpose of this cookie, along with the others mentioned here, are described below in Section 1.5.5.

1.5.5 Cookie Analysis

As part of the first audit, Facebook were asked to provide an explanation of the purpose of each of the identified cookies. The information provided at the time has been reviewed and updated as part of this audit. It was noted at the time of the first audit that Facebook uses many cookies for many purposes and it is not feasible to identify and analyse the purpose of every single cookie. Therefore, the focus of the analysis continues to be on the cookies identified in the previous sections.

Some of the cookies used by Facebook are known as session cookies. In the majority of cases, these cookies remain on the user's PC until the web browser is exited. There are a few scenarios, as mentioned in the first report, such as Firefox session restore mode where session cookies can be retained after the browser has been exited.

1.5.5.1 datr

The purpose of the datr cookie is to identify the web browser being used to connect to Facebook independently of the logged in user. This cookie plays a key role in Facebook's security and site integrity features.

At the time of the first audit, the datr cookie generation code was reviewed and it was confirmed that the execution path followed in the case of a request for social plugin content does not set the datr cookie.

The lifetime of the datr cookie is two years.

1.5.5.2 reg_fb_gate, reg_fb_ref and reg_fb_ext

The reg_fb_gate cookie contains the first Facebook page that the web browser visited. The reg_fb_ref cookie contains the last Facebook page that the web browser visited. The reg_fb_ext cookie contains an external referrer URL form when the browser first visited Facebook.

These cookies are only set when the browser is either not a Facebook user or is not logged in to Facebook. These cookies are used by Facebook to track registration effectiveness by recording how the user originally came to Facebook when they created their account.

These three cookies are session cookies.

1.5.5.3 wd

This cookie stores the browser window dimensions and is used by Facebook to optimise the rendering of the page.

The wd cookie is a session cookie.

1.5.5.4 c_user

This cookie contains the user ID of the currently logged in user.

The lifetime of this cookie is dependent on the status of the 'keep me logged in' checkbox. If the 'keep me logged in' checkbox is set, the cookie expires after 30 days of inactivity. If the 'keep me logged in' checkbox is not set, the cookie is a session cookie and will therefore be cleared when the browser exits.

1.5.5.5 lu

The lu cookie is used to manage how the login page is presented to the user. Several pieces of information are encoded within the lu cookie.

The 'keep me logged in' checkbox on the Facebook login page is used to determine whether or not the authentication cookies delivered to the user when they log in will be retained when the user quits their browser. If the 'keep me logged in' checkbox is ticked, then when the user logs in the authentication cookies will be persistent (retained after the browser exits). If the 'keep me logged in' checkbox is not ticked then the authentication cookies will be session cookies (cleared when the browser exits).

The user can explicitly check or uncheck the 'keep me logged in' box. The lu cookie records whether the user has performed such an explicit action.

If the user has not explicitly either checked or unchecked the 'keep me logged in' box, then the default mode of operation is to automatically check the 'keep me logged in' box if the same user has logged in from the same computer three times in a row without logging out. A user explicitly checking or unchecking the 'keep me logged in' box always overrides this feature.

To implement this functionality, the lu cookie contains a counter which is incremented if the user logging in is the same as the previous user that logged in from this web browser, and if the previous user did not explicitly log out. To be able to determine whether the user logging in is the same as the previous user that logged in, the lu cookie contains the user ID of the previously logged in user. The previously logged in user component of the lu cookie is set to zero if the user explicitly logs out.

The user ID component of the lu cookie is also used to pre-populate the email address field of the login form if the user did not previously explicitly log out.

To summarise, the components of the lu cookie are:

- The user ID of the previously logged in user, or zero if the user explicitly logged out.
- A counter containing the number of times in a row that the same user has logged in from this browser and has not explicitly logged out.

- A flag to indicate whether the user has explicitly either checked or unchecked the 'keep me logged in' box.

The lifetime of the lu cookie is two years.

1.5.5.6 sct

At the time of the first audit the presence of a cookie named sct was noted. This cookie contained a unix timestamp value representing the time at which the user logged in. This cookie was used to distinguish between two sessions for the same user, created at different times.

The absence of this cookie was noted at the time of the second audit and it has been confirmed by Facebook that the unix timestamp value previously contained in the sct cookie has been incorporated into the xs cookie described in the next section.

1.5.5.7 xs

This cookie contains multiple pieces of information, separated by a colon[19].

At the time of the first audit it was noted that the values contained within the xs cookie were;

- The first portion is an up-to-two digit number representing the session number.
- The second portion is a session secret.
- The third, optional, portion is a secure flag, which is used if the user has enabled the secure browsing feature.

It was noted at the time of the second audit that the xs cookie now contains four components separated by colons. The first three components are consistent with the three functions described above and the fourth component appears to be a unix timestamp, consistent with the incorporation of the value previously carried by the sct cookie into the xs cookie.

1.5.5.8 x-referer

This cookie contains the full referrer URL.

When a user clicks on a link on a web page, this leads to a HTTP request being sent to a server. The referrer is the URL of the web page on which the link that the user clicked resided. The referrer is sent with every HTTP request[20].

Facebook use this value to correctly capture the referrer for pages using Facebook Quickling navigation. Quickling navigation is a feature that uses AJAX to make Facebook page requests,

[19] Colon is encoded to the value %3A for transmission.

[20] http://tools.ietf.org/html/rfc2616#section-14.36

thus speeding up the user experience of the site[21]. In these cases, the actual referrer URL is in the URL fragment[22] and this is not normally sent to the server in the HTTP Referer[23] header.

1.5.5.9 presence

The presence cookie is used to contain the user's chat state. For example, which chat tabs are open. This is a session cookie.

1.5.5.10 p

The p cookie is known as the user's channel partition and is required by many features on the Facebook site, including chat and client-side notifications. This is a session cookie.

1.5.5.11 locale

This cookie contains the display locale of the last logged in user on this browser. This cookie appears to only be set after the user logs out and has a lifetime of one week.

1.5.5.12 lsd[24]

At the time of the first audit it was reported that the lsd cookie contains a random value that is set when a Facebook user logs out to prevent cross-site request forgery (CSRF) attacks.

Cross-site request forgery is an attack technique involving misuse of credentials from one site (in this case Facebook) to perform unauthorised actions on a user's account when the user visits a web site containing specifically crafted malicious code.

Further insight into the operation of this cookie has been gained on when this cookie is set as part of this audit. In particular, the cookie is not just set when a Facebook user logs out, rather, the cookie is set whenever the browser is in a logged out state.

The lsd cookie is a session cookie.

---

[21] Some technical detail can be found at http://www.slideshare.net/ajaxexperience2009/chanhao-jiang-and-david-wei-presentation-quickling-pagecache

[22] The URL fragment is the name given to the part of the URL after a "#" and is typically, but not always, used to refer to a part or position within a HTML document. See http://tools.ietf.org/html/rfc3986

[23] The HTTP referrer header is mis-spelled as "Referer" in the HTTP standard, so this is the correct name of the HTTP header as per the standard.

[24] FB-I reports that in the period between the time this cookie testing was performed and the completion of the report, the lsd cookie has been removed.

1.5.5.13 Cookies beginning with _e_

At the time of the first audit, it was noted that a substantial number of cookies that begin with the characters "_e_" were transmitted. These were referred to by Facebook as EagleEye cookies.

The cookie names consisted of "_e_" followed by a four character random string, followed by an underscore and then an incrementally increasing number, starting at zero. For example, _e_gh2c_0, _e_gh2c_1, _e_gh2c_2, etc.

It was reported that these cookies were generated by JavaScript and used to transmit information to Facebook about the responsiveness of the site for the user. Cookies were being used as the transport mechanism for the performance related information, but the content of the cookies was being generated in the user's web browser and no information was being transferred to Facebook that was not available for transmission in some other form (e.g. in a HTTP POST). Facebook did not place any information on the user's PC using these cookies.

It was further noted that it was possible to observe, by monitoring the communication between the web browser and Facebook, that each time an EagleEye cookie was submitted to Facebook, the corresponding response unset that cookie. This is consistent with the explanation provided by Facebook that these cookies are used as a transport mechanism.

The EagleEye cookie value consisted on an encoded JSON structure that contained information about an action performed by the user on the site. For example, when the user clicked on a link.

The testing carried out as part of this audit revealed that _e_ cookies are still in use and their behaviour continues to be as described here.

1.5.5.14 fr

As part of the testing carried out for this audit, a new cookie named fr was identified.

It was noted that the cookie is only set when a Facebook user logs in to the site and it has an expiry period of 30 days. The cookie, including the encrypted user id, is retained after the user logs out. Upon examination, the fr cookie clearly consists of two components.

An example fr cookie value is "0nx07ppspaoOQlQv1.AWVAlyAiGNl9vuExmcrX2lmfAfk".

Facebook were asked to provide an explanation of the purpose of this new cookie.

The content of the two parts of the cookie have been reported to be as follows;

- The first part of the cookie is a browser ID, used to identify the web browser.
- The second part of the cookie is an encrypted version of the logged in user's Facebook ID. The user's ID is re-encrypted every hour to a different value.

The code used to generate the fr cookie value has been reviewed and it has been confirmed that the browser ID is a random value and the encrypted user ID value contains only the Facebook user ID. It was also confirmed by code review that the fr cookie value generation code is called whenever the other login session cookie values (c_user, xs, etc.) are refreshed, which takes place roughly hourly but this can vary for operational reasons.

This cookie is being used by Facebook to deliver a series of new advertisement products such as real time bidding, which works as follows:

- An advertising partner of Facebook, for example, doubleclick has an ad on, for example, the New York Times website[25].
- A Facebook user visits the New York Times.
- The website contains a pixel image which causes a request to be sent to Facebook. Usually, the request to Facebook will have a referrer value of the partner (in this case doubleclick), along with an opaque partner value provided by doubleclick. In some cases, partners do not control the browser referrer value. In such cases, FB-I states that they exclude this referrer value from their impression logs and do not use it as part of this or other advertising systems.
- Facebook store a relationship between the partner value and the fr cookie browser component value.
- Then, when the user visits Facebook, the partner is sent the partner value and can respond with a bid amount to bid to have an ad displayed to the user.
- If the partner wins the bid, Facebook will serve a standard ad from a standard ad campaign to the user.

To summarise what each of the actors know about the user's activity:

- The partner (doubleclick in this case) knows that the user has visited the New York Times website.
- Facebook do not know that the user has visited the New York Times website[26]. The meaning of the partner value provided to Facebook is opaque to Facebook. FB-I report that the partner values are typically short identifiers. While this value may, hypothetically, somehow encode the fact that the user has visited the New York Times website it is not clear how or why the partner would choose to do this. The partner will store whatever data they know about the user in their own database.

[25] With the exception of Facebook, the actors described in the following example are intended purely to illustrate the functionality of the cookie. It is not known, nor is it relevant, whether doubleclick is an advertising partner of Facebook or whether doubleclick have an ad on the New York Times website.

[26] As mentioned above, sometimes FB-I may receive this value in a HTTP referrer header but they have stated that they do not log the referrer value from such requests.

- Facebook know information about the user provided separately by the user to Facebook (e.g. the user's profile information).
- The partner has no access to any information provided by the Facebook user to Facebook.
- Due to the bid requests, the partner may know which browsers are active Facebook users, but they are contractually prohibited from storing or using this fact.

Although this cookie will be sent in requests for social plugins that occur after a browser has had a logged in user, FB-I states that this cookie is not currently used other than as described above.

1.5.5.15 sub

During the testing for this audit, the presence of a cookie named sub was noted. This cookie was not present at the time of the first audit. The value of the sub cookie was noted to be a simple numeric value but Facebook were asked to clarify the purpose of this new cookie.

The chat functionality on the Facebook site works using a technique known as HTTP long polling[27]. This technique involves the client sending a HTTP request to the chat server and the server holding the connection open by taking a long time to respond to the request.

This leads to a situation where, if the user has multiple tabs open, there are multiple simultaneously open HTTP connections to the same server. Most browsers limit the number of allowed simultaneous connections (typically to a value somewhere in the region of six).

The sub cookie is used by Facebook's chat JavaScript to communicate across tabs to coordinate connections to the Facebook chat server. The sub cookie replaces an older, less effective technique for addressing the same issue.

1.5.6 Active Cookie Management

As part of the first audit, Facebook demonstrated a feature for proactive management of browser cookie state, known as "Cookie Monster".

The cookie management framework contains configuration for each cookie and the context in which the cookie should be set. For example, certain cookies are required in the context of a logged in user and after the user logs out these cookies should be unset. If a cookie is received for which there is not a configuration, it will automatically be cleared.

The cookie management framework is executed on every Facebook request, including requests from social plugins. Unexpected cookies, or cookies from the incorrect context (such as cookies that are only meaningful in the context of a logged in user being received in a request from a non-logged in user), are automatically unset.

[27] http://en.wikipedia.org/wiki/Push_technology#Long_polling

Several tests were performed where invalid cookies and cookies in the incorrect context were passed to Facebook in HTTP requests and it was noted that all unexpected cookies are cleared in the next response received. For example;

- A c_user cookie value was added to a HTTP request for the Facebook home page with no user logged in. The c_user cookie is only meaningful in the context of a user being logged in to Facebook and therefore this cookie was cleared by Facebook.
- A random cookie ("blah=blob") was added to a HTTP request for the Facebook home page with no user logged in. The "blah" cookie is not meaningful to Facebook and therefore this cookie was cleared by Facebook.

Facebook highlighted several scenarios where the cookie management framework will not clear cookies. These are:

- Cookies with invalid names. Facebook does not set any cookies with invalid names.
- Cookies that Facebook believe will not be cleared upon request (e.g. data in the form of cookies inserted into the cookie header by a mobile carrier WAP gateway).
- It is possible for a user to manually craft a cookie in their browser that will be sent to Facebook which Facebook is unable to clear because the parameters used to set the cookie (e.g. the cookie path) are not known.

Finally, it was reported that due to the asynchronous nature of Facebook's architecture, it is possible that a response has been sent to the user before the cookie checks have been completed or before the login state of the user is known. In these cases, the cookie management will occur on the next appropriate request. It was concluded that within the lifecycle of a single browser interaction with Facebook, the Cookie Monster code will always be run.

The cookie management framework code has been re-reviewed as part of this audit and confirmed to continue to operate as described in this section.

1.5.7 Non-Cookie Information

As noted in the first report, as well as cookie information as described above, other HTTP information is transmitted along with requests for social plugins. In particular;

- The HTTP headers sent by the web browser[28]. Typically these include;
    - The Accept header: content formats that the web browser can accept.

[28] The headers mentioned here are only intended as a summary of the typical information provided in typical HTTP headers. Full details of the possible headers can be found in the HTTP standards.

- The Accept-Language header: content languages that the web browser can accept.
- The User-Agent header: typically contains the type of browser software and the operating system.
- The Accept-Encoding header: whether the web browser can accept compressed responses, and in what format.
- The Host header: The hostname for which the HTTP request is being made.
- The Connection header: allows the sender to specify options that are desired for the particular connection. For example, whether to keep open or close the connection after the request has been processed.
- The Cookie header: contains cookie values.

- Time and date of the request
  - The time and date that the Facebook server received the request.
- Browser IP address
  - Performing a HTTP request involves setting up a connection between the PC on which the web browser is running and the Facebook server that will process the request. Establishing such a connection requires that the server must know the IP address being used by the client[29].

Nothing has changed in the intervening period to alter this finding and Facebook will necessarily continue to receive the information listed above as an effect of processing HTTP requests.

1.5.8 Logging

During the first audit Facebook were asked to provide a list of all queries run against social plugin logs over a period of a month. These queries were analysed to assess the nature of the queries performed and in particular to determine whether any queries for the activity of individual users were performed.

In the first audit, a spreadsheet of almost 3,000 queries was provided and it was noted that:

- Only a single query was identified containing individual object IDs. Each of the individual IDs were investigated and all turned out to be IDs of Facebook pages.
- Facebook employees create database views of the raw data set in order to more efficiently query certain portions of the social plugin logs. All queries identified in the spreadsheet that queried such views resulted in aggregate data being returned.

It was therefore concluded at the time of the first audit that, whilst not conclusive, there is no evidence in the information presented that individual user or non-user browsing activity is being extracted from social plugin logs for analysis.

[29] As mentioned in the first report, certain scenarios exist where the browser is not making a direct TCP/IP connection to Facebook. The most notable examples are the use of NAT (Network Address Translation) and the use of a web proxy. In these cases the IP address received by Facebook will not necessarily be the same as the IP address of the browser's PC.

During this audit, all social plugin queries performed during a second random month long period were examined. A total of 2,107 queries were examined. All individual object IDs (210 in total) were examined and it was confirmed that none represented Facebook users.

It is therefore concluded that the examined information continues to indicate that no individual user or non-user browsing activity is being extracted from social plugin logs for analysis.

1.5.9 Use of Social Plugin Activity to Target Advertising

During the first audit, testing was performed to establish whether interacting with websites containing social plugins would influence the advertising that the user was presented with. It was concluded that:

- The act of browsing to websites containing social plugins does not appear to have any influence on the advertising targeted at a user.
- Pressing the “Like” button either on a Facebook page or on a page with a social plugin may influence the advertising presented to the user.
- The advertising targeting appears to be focussed on particular Facebook pages and/or very specific keywords.
- Behavioural profiling was not evidence in the findings. Browsing a category of websites or interests (e.g. parenting/childcare or motorcycles) did not appear to have any influence on the advertising targeted at the user. It is possible that other advertisements may use broader categories or keywords but none were identified at the time of the testing.

This testing was repeated as part of the second audit, and the behaviour was found to be consistent with the above findings.

It is perhaps important to re-emphasise that great care is required in the setup and execution of this testing because there can be many confounding factors. In particular, advertisements can be targeted using very specific criteria, to include factors such as geographic location, age or gender of the Facebook user. Therefore, it is important to ensure that all Facebook accounts used for testing in this regard are consistently configured and the only difference between the accounts is the browsing activity being considered as part of the test. To remove any complexity that may be introduced by the activity of friend’s Facebook accounts, it is further recommended that all testing accounts have no friends.

1.6 Akamai Cache

In order to facilitate faster loading of the Facebook page, static content such as images and JavaScript files are cached using the Akamai caching service. 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.

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 them.

1.6.1 Predictability of Akamai Cache URLs

An example filename given by Facebook to an image file is:

https://fbcdn-sphotos-a.akamaihd.net/hphotos-ak-ash4/387755_115906941856985_100003130400274_87779_1581190684_n.jpg

As described in the first report, the Akamai cache URLs consists of five numeric components as follows:

- The volume ID: The first number is an identifier for the physical Facebook server where the image is located.
- The Facebook object ID: The second number is a unique identifier for the photo.
- The User ID: The third number is the User ID of the user who uploaded the photo.
- The Photo ID: The fourth number is a legacy photo ID. For newer photos this value is ignored. Specifically, if a Facebook object ID is provided, the Photo ID is ignored.
- The fifth number is a pseudo-random number to make the URL unpredictable.

During the first audit an assessment of the strength of the randomness used to generate random component of the URL. This directly influences the ability of an individual to generate photo file names for photos that they did not previously have access to.

To achieve this goal, the volume ID, Facebook object ID, user ID and random number component are all required. Based on the analysis carried out in the first audit it was concluded that

1. The technique used to generate pseudo-random numbers is of sufficient strength that it is not possible to guess the random component of an arbitrary photo file name.
2. The easiest way to have the volume ID, Facebook object ID and user ID corresponding to a particular photo 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.
3. In the case where an attacker does not have access via Facebook to a target image; even it were possible to guess the value of the pseudo-random number, this will not help to recover the volume ID or Facebook object ID of the image, regardless of whether the target user ID is known.

It was therefore concluded 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.

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

1.6.2 Deletion of Facebook Photo

After a user has deleted a photo, Facebook no longer serves the photo. However, Akamai will have cached a copy of the photo and therefore continue to return the deleted photo for a period of time. Facebook report that the Akamai cache will retain the deleted content for a maximum of 30 days.

To confirm that Facebook no longer serves the photo after the user has deleted it; a cache bypass technique was used. This involved appending arbitrary strings to the end of the photo URLs. The Akamai cache cannot match the different text string with the original image and will therefore revert to Facebook to get another copy of the image. If the photo has been deleted, this new URL will fail to return the image, even though Akamai has cached the deleted photo under the original URL.

For example, suppose the following image URL represents an image on a user's Facebook wall; https://fbcdn-sphotos-a.akamaihd.net/hphotos-ak-ash4/387755_115906941856985_100003130400274_87779_1581190684_n.jpg. By appending a random query string, such as "?a=b" to the end of the URL, Akamai will request a second copy of the image from Facebook. If the user has deleted the photo from their wall, this request will fail to return the content of the image.

The original URL will continue to provide the photo for up to 30 days, since the photo has been cached in Akamai, but Facebook no longer provide this URL whenever anyone visits the wall of the user who deleted the image. Unless a user who had previously viewed the image already knew the URL, it is not possible to predict this URL and retrieve the cached copy, as discussed in Section 1.6.1.

This testing has been re-performed as part of this audit and the results described above have been replicated.

1.7 Scraping

Scraping, also known as screen scraping, is the name given to an automated process of harvesting data from a website. In the case of Facebook, the concern surrounds the ability of an automated process to gather a large volume of information about Facebook users.

As part of the previous review, FB-I provided details of the arrangements they have made to prevent scraping. It was concluded that the arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data while allowing service to be effectively provided to legitimate users in a wide range of circumstances.

Facebook have confirmed that the arrangements to prevent scraping are still in place and have not changed since the last review.

1.8 Account Creation Cancellation

In the previous technical report an issue was considered concerning a new user who begins the Facebook registration process but does not complete the registration. At the time, there was a particular concern surrounding the fact that the user may have populated the registration form with their name, e-mail address, gender and date of birth. This information was submitted to Facebook and then the user was presented with a CAPTCHA. It was only this point that the user was presented with an opportunity to read the terms of use and privacy policy.

FB-I reported that if a user cancelled their registration in this way an automated process would delete the provided information within 30 days. A code review was performed to confirm that the code of this automated process operated as specified, deleting all information stored when the user filled in the first page of the registration.

In the intervening months, Facebook have redesigned the registration process, which no longer consists of two steps as described above. There is therefore no information stored about individuals who abandon the registration process. Prospective users have the opportunity to view terms of use and privacy policy on the Facebook front page before beginning their registration.

1.9 Account Deletion

Facebook users can choose to either deactivate or delete their account.

If a user deactivates their account, this means that the user's profile information will not be available on Facebook, effective immediately. However, Facebook retains the users information indefinitely in case the user chooses to reactivate their account at some point in the future.

Deletion, on the other hand, leads to the permanent removal of the user account from Facebook.

1.9.1 Account Reactivation

The question was asked during this audit how many people either reactivate their account after deactivating it or return to their account after not having logged in for an extended period of time. A sample date was chosen and the number of users who reactivated their account or returned to their account after not having logged in for three years or more on the day were calculated.

On the date chosen, which was 1st July 2012, 733 users reactivated their accounts and 11,818 users logged in after being away from the site for more than three years. To confirm that at least some of these were real users a small random sample of the accounts were examined and it was verified that the accounts appeared to show patterns of genuine activity.

1.9.2 Deletion Framework

The first report briefly described the deletion process as follows:

- After a user submits a request to delete your account, the account enters a state of "pending deletion" for 14 days. During these 14 days it is possible for the user to change their mind and cancel the deletion. This 14 day period is provided for various reasons, including allowing a user "cooling off "period and also to cater for the case where someone with unauthorised access to a user account issues a delete instruction.
- If the user logs into their accounts during the 14 day period where the account is pending deletion, they are presented with a message stating "Your account is scheduled for deletion. Are you sure you wish to permanently delete your account?". The user can then either confirm or cancel the deletion process.
- Once the 14 day period has expired, an account deletion framework is activated which deletes the account information.

The account deletion framework was briefly discussed in the first report. As part of the second audit, the deletion framework has been extensively studied and reported on below.

The main areas where user data is stored, which have been examined as part of this audit, are:

- UDBs: The user databases where user account details and much user generated content is stored.
- Hive: Used for log storage.
- Haystack: Primarily used for storing photos.
- Titan: Message storage for private messaging.

Each of these has been examined in turn to understand how Facebook verifiably delete data from these locations.

1.9.2.1 UDB Data

Much user content is stored in user databases, referred to as UDBs.

Historically, users were represented by entries in an "info" table, the primary identifying table for users, which contained the user's username, password and other basic account information. The specific database that contains a particular user's "info" table entry is referred to as that user's local or home database. The local database also contained a "friends" table that stored the friend relationships of users in the corresponding "info" table. Feature specific tables were used to store data generated through user interaction with a particular site feature.

This model has been largely replaced with a general model of objects (referred to as FBObjects, identified by a unique ID referred to as an FBID) and associations (referred to as assocs) between those objects. In this new model a user is represented by and FBID and the user

information previously stored in the “info” table is stored in an FBObject associated with the user’s FBID. This FBObject is referred to as the user object.

As mentioned above, 14 days after a user requests the deletion of the account the account deletion takes place. The deletion framework is invoked to recursively delete all information associated with the user's account.

The deletion framework consists of a deletion coordinator and a range of deleters programmed to delete a certain type of user information. The role of the deletion framework is to ensure that each of the required deleters complete successfully.

Each of the deleters can call other deleters as required to recursively delete data. A requirement is placed on all Facebook developers that are developing new features for the site to develop a deleter that will remove user content generated by users of that feature. The developers are provided with access to a library of primitive deleters, which can be thought of as deletion building blocks, to perform low-level deletions in both of the data models described above. A non-exhaustive, representative list of the primitive deleters is:

- UDBRowDeleter: deletes a single row from a UDB table in the historical model described above.
- UDBRowIteratingDeleter: deletes all rows of a certain type from a UDB table in the historical model described above.
- FBObjDeleter: deletes an FBObject.
- SingleAssocDeleter: deletes one assoc of a certain type.
- AllAssocDeleter: deletes all assocs of a certain type.
- AssocRecursiveDeleter: Deletes an assoc of a certain type, and run the deleter of the provided type on the FBObject at the far end of the assoc. This is used to recursively delete FBObject structures.

As mentioned in the original report, after the account has been deleted, the fact that an account with a particular user ID has been deleted is recorded. Specifically the following information is retained:

- The user ID of the deleted account
- The status of the account is deleted
- The time and date when the account was deleted

This information is retained for several reasons:

- To allow Facebook to be able to distinguish between the case of a user ID that has never existed and a user ID that used to exist but has been deleted.
- To enable Facebook to re-run the deletion process on the account in order to remove additional information that was missed when the account was originally deleted.

As mentioned above, the user object stores the basic information for the user. If the user object were deleted there would be no record of the fact that the account used to exist but if the user object is not handled in some way by the deletion framework the account deletion could not be considered complete. Therefore, two additional primitive deleters have been developed specifically to handle the user object;

- UDBRowOverwritingDeleter: this deleter zeros out all columns in a row except for those listed in the deleter's configuration. This deleter is used remove data from the "info" table for accounts stored using the historical data model.
- FBObjOverwritingDeleter: this deleter performs the same task as the UDBRowOverwritingDeleter in the newer data model.

When the developer has completed the deleter for their new feature, it will be invoked whenever a user subsequently deletes their account. At the time of writing, 168 individual deleters are directly invoked by the UserPermanentDeleter, the top-level deleter called by the deletion framework to delete a user account. Since deleters are built upon layers of other deleters, there are 448 deleters in total.

It was noted that the final deleter executed by the UserPermanentDeleter identifies any remaining data not deleted by any of the other deleters and automatically raises a high priority task, which is assigned to the engineers working on the deletion framework, to manually investigate the remaining data and develop additional deleters as required. When the deletion framework is rerun, the newly identified data will be deleted for all previously deleted user accounts as well as any accounts newly pending deletion.

There have been several instances where Facebook's deletion framework has, due to software bugs for example, deleted information that should not have been deleted. Therefore, the deletion framework has a built in recovery feature to protect against these cases and to allow restoration of data deleted in error. The recovery feature works as follows:

- When the deletion coordinator executes a deleter, a deletion FBObject is created and associated with the object being deleted and a reference to the deletion FBObject is entered into a table called assoc_deletion (for deleted assocs) or fbobj_deletion (for deleted FBobjects).
- A serialised version of the object or association being deleted is stored in the deletion FBObject.
- No code other than the deletion framework is able to access or restore the serialised version of the deleted data. The restoration of the serialised data must be performed manually.
- The serialised version of the deleted data is deleted after 14 days.

Facebook's internal testing framework for code acceptance automatically performs aggressive testing on all deleters. In particular,

- The testing framework executes the deleter and ensures that everything expected to be deleted is deleted and everything expected to be untouched is untouched.
- The testing framework runs the delete in reverse and ensures that everything is restored to the original state.
- The testing framework re-runs the deleter, interrupting the deleter after every mutation to ensure that the deleter restarts and completes successfully.
- The testing framework re-runs the deleter in reverse, interrupting the deleter after every mutation to ensure that the deleter completes the restore successfully.

1.9.2.2 Hive Data

Hive is the name given to Facebook's log storage area. It is based on the Hadoop platform[30]. Data stored in hive is organised logically as tables which are split into partitions, mostly by date. Partitions are then divided out among multiple physical nodes within hive. For redundancy, three copies of data are stored.

The fact that the data is stored in hive organised by date presents a challenge in the context of account deletion. There is no way to extract all log entries corresponding to a particular user account without searching all partitions for all dates. The act of deleting these entries, once they have been located, would involve rewriting every single partition that contained entries relating to that user[31].

1.9.2.2.1 Table Retention Policies

In order to circumvent this computational challenge, FB-I configure a data retention policy for each table in hive. It is the responsibility of the table owner to set an appropriate retention policy for their tables. Tables automatically have older data pruned as the age of the data moves beyond the retention period. A distinction is made between data that will be retained for less than 90 days and data that will be retained for more than 90 days;

---

[30] http://hadoop.apache.org/

[31] The following analogy may help clarify the computational difficulty of deleting user activity logs from hive; imagine a table partition in hive as a telephone book. The entries in telephone books are organised alphabetically in the same way as the entries in hive are organised by date. Suppose you wanted to delete all entries from the phonebook corresponding to a particular postal address. Locating the appropriate entries would involve searching the entire phonebook from start to finish, checking the address of each entry to see if it matches target postal address. Continuing with the analogy, the task of deleting a user's log activity from the hive would be equivalent to removing entries from a phone book by transcribing the entire telephone directory while omitting the entries corresponding to the target address. Now imagine having to repeat that process with 100,000 telephone books and the computational challenge of removing even a *single user's* activity logs becomes clear.

- Tables with a retention policy of 90 days or less are not required to have a configured UII policy.
- Tables with a retention policy greater than 90 days must have a configured UII (user identifying information) policy, which is used to remove user identifying information from table entries greater than 90 days old. Any information which could be used to identify the user and all user generated content must be anonymised after 90 days[32].

UII policies specify how each column in the table should be anonymised. Two broad categories of UII policies are available referred to as “stock anon” and “complex anon”. The “stock anon” policy is used in most cases but the “complex anon” allows for more sophisticated rewriting of table entries.

1.9.2.2.2 Stock Anon UII Policy

In the “stock anon” case is possible for the table owner to configure several possible actions for each column in the table, such as:

- keep: a policy of “keep” for a particular column means that the column does not contain any user identifying information and the value of the column does not need to be changed after 90 days.
- wipe: a policy of “wipe” for a particular column means that the column contains user identifying information and the value of the column should be wiped after 90 days.
- uid2rid: a policy of “uid2rid” for a particular column means that the column contains a user ID. After 90 days user IDs are replaced with a replacement ID value that is associated with the user's account until deletion. See Section 1.9.2.2.4 for more detail.
- browsercookie: a policy of “browsercookie” for particular column means that the value of the column represent a user's browser (datr) cookie. Certain safety and security features of the site require analysis of the value of the browser cookie. The browser cookie value is replaced with a hash of the browser cookie value combined with a secret key. The secret key is changed every 10 days. The same cookie value will only map to the same replacement value for 10 days and there is no way to meaningfully compare the replacement values from two different 10 day windows, where the cookie values have been hashed with two different secret keys. This means browser cookie analysis can only be performed over a 10 day window once the log entries are more than 90 days old. Hashing is not considered sufficient for anonymisation of user IDs but it is believed to be sufficient in this case. Since there are a (relatively) small number of known user IDs, in the single-billions region, it would be hypothetically possible to re-map a hashed value into the range of known user IDs. The fact that browser cookies already include a 64-bit random number combined with the 10 day rotating secret key effectively removes the ability to re-map replacement browser cookie values to the original values.

[32] This includes in particular UIDs, IP addresses, DATR cookie values, email addresses, phone numbers, names, addresses and any user generated content including text of status updates.

1.9.2.2.3 Complex Anon UII Policy

There are certain cases that require a greater level of rewriting sophistication than can be provided by the "stock anon" policy described above. Two examples where this is the case are:

1. Structured column values, such as where a table column contains a JSON[33] value. In these cases, only certain values within the JSON structure may contain user identifying information and so the stock anon "keep" policy would not be sufficient but the stock anon "wipe" policy would be excessive. Therefore, the complex anon policy allows specification of a sub-policy that can be applied to individual values within a JSON structure.

   Using a concrete example to clarify, consider the JSON structure {"uid":12345, "colour":"red", "email":"a@b.com"}. In this case, a column policy of (uid, uid2rid, colour, keep, email, wipe) would mean that the uid value will be replaced with the corresponding replacement ID, the colour will be kept and the email value will be wiped.

2. Column values that contain URLs where certain components of the URL are user identifying. In these cases, similar to the scenario just described, the stock anon "keep" policy would not be sufficient but the "wipe" policy would be excessive. Therefore, there is a "url" policy that can be used to specify a regular expression that can be used to rewrite the URL. URLs may also contain other URLs encoded within them, so url policies can be applied recursively. Additionally, certain parameters within URLs that are known to contain user identifying information will automatically be wiped as will any appearance of the authenticated user's id in decimal form (the form common in Facebook logs).

   Considering the example "profile.php?id=12345" where the id parameter contains a user ID. In this case, the "url" policy regular expression could be used to replace the user ID with the corresponding replacement ID for that user.

1.9.2.2.4 UID to RID mapping

The rewriting of user IDs with replacement IDs is fundamental to FB-I's ability to de-identify log file entries when a user deletes their account. As mentioned above, when a user requests that their account be deleted, it is computationally infeasible for FB-I to delete all log entries associated with the account activity. However, by deleting the relationship between a user ID and the associated replacement ID whenever a user deletes the account, FB-I de-identify the corresponding log entries to the extent that it is no longer possible to associate the log records with the deleted account.

A substantial amount of time has been expended by FB-I to develop a scheme for generating replacement IDs. It is a requirement that it is not possible to reverse engineer the original user ID from the replacement ID or to infer anything at all about the user from the replacement ID. At the same time, the scheme must remain consistent over time. Several hash based techniques were considered. As mentioned briefly in Section 1.9.2.2.2, hash based techniques are vulnerable to re-mapping of the hashed value back to the range of known user IDs. Considering the efficiency

[33] http://en.wikipedia.org/wiki/JSON

of modern hash functions (a common laptop can compute more than 1 million hashoperations per second), hashing alone is not considered sufficient for data de-identification. Ultimately it was determined that the optimal solution was a one-to-one mapping between a user ID and a replacement ID, where the mapping is deleted on account deletion.

Replacement IDs are a type of FBID (mentioned in Section 1.9.2.1). Since FBIDs have internal structure, they could reveal information about the user such as which user database the user's information is stored on. Therefore, the standard scheme for generation of new FBIDs was not considered appropriate and a separate scheme that does not leak any information about the user was created.

The mapping between the user's ID and the replacement ID are stored as an assoc (see Section 1.9.2.1) between the user FBObject and the replacement FBID. It has been confirmed by code review that a deleter called UserRidDeleter, which deletes the user ID to replacement ID mapping, is called by the UserPermanentDeleter. Recall the UserPermanentDeleter is invoked by the deletion framework 14 days after a user requests account deletion. See Section 1.9.2.1 for more detail of deletion of user information from UDBs.

1.9.2.2.5 Performing the Rewriting

To perform the log de-identification rewrite, all of the user ID to replacement ID mappings must be extracted from the UDBs and placed in hive. Previously, an entire dump of all user ID to replacement ID mappings was performed every day. This turned out to be too computationally intensive on the UDBs and therefore this system has been replaced with 10% of all mappings being extracted each day and aggregated into a single location in hive. Changes, such as newly created user ID to replacement ID mappings are also pushed to hive and aggregated into the same location.

In the early versions of the rewriting code, the mapping was performed by joining[34] a table containing the log entries to be rewritten to a table containing the user ID to replacement ID mappings. The resulting rows were the rewritten log entries. This turned out to be extremely inefficient and also could not handle sub-column ("complex anon") policies.

Therefore, a second solution was developed which involved the creation of a separate index server that contained the user ID to replacement ID mappings. Functions could then be built which queried the index server for specific user ID to replacement ID mapping values rather than joining the entire table of user ID to replacement ID mappings. This turned out to have a substantial network I/O bottleneck while querying the index server so this system was enhanced by developing a batching system to accumulate a group of rows to be rewritten, up to a limit defined by a memory threshold, and then sending a query for a batch of user ID to replacement ID mappings to the index server. This led to a substantial increase in rewriting efficiency.

[34] http://en.wikipedia.org/wiki/Join_%28SQL%29

FB-I have undertaken to ensure that all log entries in hive have been de-identified within 90 days, including having all user IDs replaced by the replacement ID. Several sample tables have been reviewed to confirm that the rewriting process is complete after 90 days and in all cases examined, rows older than 90 days in tables with retention greater than 90 days had been de-identified.

It has been confirmed by FB-I that the entire hive logs have been fully rewritten and de-identified as described in this section. Internal reports on the progress of the rewriting have been viewed and it has been noted that, according to the reports, the percentage of historic hive logs remaining to be rewritten is now zero.

1.9.2.2.6 Exceptions to Rewriting

FB-I have stated that there are three types of tables where data is not rewritten as described here;

- Business records stored in Hive but marked as "anonexempt". These tables contain no personal data for users or non-users. Examples include:
    - Aggregate statistics of network traffic volumes by major netblocks or Autonomous System Number (ASN). Because the IP address and network numbers included in this table are aggregated by network, they do not need to be deleted as they do not identify any person.
    - Impression logs local to FB-I's internal network, which are used to monitor FB-I employee access to the site for work purposes. These logs do not contain the personal data of users or non-users.
- Log data on legal hold, for example, where FB-I has been ordered to hold data in its original form due to litigation. This data is held separate from Hive, where it is not accessible for analysis in Hive nor accessible to the log rewriting process.
- Log data held to meet FB-I's obligation for financial audit reporting. This data is held separate from Hive, where it is not accessible for analysis in Hive nor accessible to the log rewriting process.

1.9.2.3 Haystack Data

Haystack is a raw binary data store used by Facebook to store, amongst other things, user uploaded photos. Facebook have published a summary of the operation of Haystack which can be found at https://www.facebook.com/note.php?note_id=76191543919 . To briefly quote some of the salient points from this article;

- *"The main aim of Haystack is to eliminate unnecessary metadata overhead for photo read operations."*
- *"The delete operation is simple – it marks the needle in the haystack store as deleted by setting a 'deleted' bit in the flags field of the needle. However, the associated index record is not modified in any way so an application could end up referencing a deleted needle. A read operation for such a needle will see the 'deleted' flag and fail the operation with an appropriate error. The space of a needle is not reclaimed in any way.*

The only way to reclaim space from deleted needles is to compact the haystack (see below)."

- *"Compaction is an online operation which reclaims the space used by the deleted and duplicated needles (needles with the same key). It creates a new haystack by copying needles while skipping any duplicate or deleted entries. Once done it swaps the files and in-memory structures."*

FB-I identified an issue with the deletion mechanism as described here. Suppose the compaction process takes place once every 30 days. If an item is deleted on day one of the 30-day cycle, it will be available for recovery for 29 more days. However, if the item is deleted on day 29 of the 30-day cycle, it will only be available for recovery for one day. FB-I confirm that this implies that a file deleted on day 1 of the cycle will not be deleted until 59 days later; the remainder of the current cycle plus one full cycle.

This raised issues where accidental deletions were unrecoverable due to the 29th day scenario just described. Therefore, a modification to the deletion process has been added to ensure that deleted items are available for at least one full compaction interval. When items are deleted they are now marked with a timestamp as well as the deleted flag to ensure that only objects marked for deletion sufficiently long ago are deleted.

1.9.2.4 Titan Data

Titan is the name of the Facebook private message storage area. Interactions with the titan storage area can take place via the Facebook website, for example via interactive chat and via Facebook email. Incoming emails for Facebook users are also stored in Titan.

Messages are stored in Titan using HBase[35]. The architecture of HBase consists of a number of cells, with a fraction of users allocated to each cell. There is no association between the data stored in separate cells. To clarify this point, consider the case of user Alice sending an email to user Bob where Alice's messages are stored in cell A and Bob's messages are stored in cell B. When Alice sends the message to Bob, the copy of the message stored in her 'Sent' messages will be stored in cell A and the copy of the message stored in Bob's 'Inbox" will be stored in cell B. The point being that two copies of the message are stored, one in Alice's cell and one in Bob's cell.

If Alice subsequently deletes her account, the copies of all of her messages are deleted from Titan. Bob's copy of the email will not be deleted when Alice deletes her account. This is as one would expect with an email service.

Titan also supports message attachments but they are handled differently. The message itself is stored in Titan but the attachment itself is stored in haystack (see Section 1.9.2.3) with a reference to the haystack location stored in Titan along with the message.

[35] http://hbase.apache.org/

Since there is no association between cells, the problem that now arises, within the context of account deletion, is how to know when the last reference to the attachment has been deleted, and therefore whether to delete the attachment. Using the example above; when Alice deletes her account, if Bob has a copy of a message with an attachment from Alice it would not be appropriate to delete the attachment when Alice deletes her account because that would delete Bob's copy.

Centralised reference counting is a possibility but that option was dismissed by FB-I as being too operationally unreliable in practice, considering the particular quirks of the technologies in question. Another alternative would be to scan all other cells in Titan to determine whether any other references to the attachment are left. This would remove the advantage of the fact that there is no association between cells.

Therefore, the solution that has been implemented is that when the attachment is being stored in haystack, it is encrypted using 256-bit AES and a copy of the key is stored with each copy of the message. This means that when the last copy of the message is deleted there is no way for anyone to retrieve the content of the attachment because all copies of the decryption key have been deleted. At the present moment, this system means that the space in haystack is permanently leaked.

1.9.2.5 Group Content Deletion

At the time of writing, when a user deletes their account any content that the user has added to a group will not be deleted, but that this data is not visible on the site. The data is tied to the deleted author's user ID so that it can be correctly deleted when the functionality described below is complete. All other personal data associated with the author will have been deleted when the account is deleted.

Currently, to identify all of the group posts created by a user account would involve searching every single group on the Facebook site and checking whether the user to be deleted had added any content to that group. This is computationally infeasible considering the large volumes of data involved.

FB-I are working on a new data model that will enable the deletion of group content when accounts are being deleted. This is due to be finished in early 2013. When the new functionality is launched, all accounts that have previously been deleted will be re-deleted and therefore all group content associated with all deleted accounts will be removed at that time.

2 Part 2: Additional Testing

Several additional features that were not examined as part the first audit were examined during this audit. The second part of this report provides details of the additional testing carried out and the results thereof.

2.1 Accessibility of User Browsing Activity Log Entries

The question of how difficult would it be for Facebook to examine an individual user's browsing activity log entries from Hive (c.f. Section 1.9.2.2) was considered.

User browsing activity log entry data is stored by Facebook in a storage area known as hive, described above in Section 1.9.2.2. As mentioned above, data stored in hive is organised logically as tables that are split into partitions, mostly by date. Partitions are then divided out among multiple physical nodes within hive. For redundancy, three copies of data are stored.

The fact that the data is stored in hive organised by date means that there is no efficient way to extract all log entries corresponding to a particular user account. To achieve this goal would involve searching all partitions for all dates from the current date back to the inception of Facebook's hive for a particular user ID.

Additionally, FB-I only stores logged out and non-user social plugin impression logs for ten days. The deletion of logged out and non-user social plugin impression logs after ten days has been verified by code review. The logged in social plugin impression logs are deleted after 60 days and this has also been verified by code review.

Considering the volume of data stored in hive, this search is considered computationally infeasible even for one single user account, let alone for wholesale reconstruction of user activity.

2.2 EXIF Data in Uploaded Images

Exchangeable Image File Format (EXIF) data provides a way to store metadata about, for example, a photo within the image file itself[36]. This can include date and time that the photo was taken, the make and model of the camera and the height and width of the image. The EXIF data may also contain the GPS coordinates at which the picture was taken.

Testing was performed to determine what, if any, processing Facebook perform on the EXIF data of an image before serving that image to users of the Facebook site.

[36] http://en.wikipedia.org/wiki/Exchangeable_image_file_format

A photo was taken using an iPhone and it was confirmed that the EXIF data contains the make and model of the iPhone, the date and time that the picture was taken as well as the GPS coordinates at which the image was taken. A test Facebook user account was used to upload the photo to Facebook and a copy of the photo was downloaded from the Facebook site. The EXIF data of the image served by Facebook was examined and it was noted that all identifying information has been removed from the EXIF data.

In particular, it has been confirmed that the information listed above (make and model of camera, time and date of creation of image and GPS coordinates) has all been removed from the version of images presented to users of the site.

2.3 Facebook Advertising

When an advertiser creates an advertising campaign on Facebook, the data relating to the campaign is visible through Facebook's ad manager interface.

The details of the information an advertiser can view have been examined and it has been confirmed that there is nowhere that has been identified within the ad manager interface where it is possible for an advertiser to identify any details of an individual Facebook user who has clicked on their ad.

It is possible for the advertiser to generate several reports as follows[37]:

- Advertising Performance: "This report includes statistics like impressions, clicks, click-through rate (CTR) and spend. Although this information is available in your Ads Manager, you may find this a useful way to export and manage your Facebook performance."
- Responder Demographics: "This report provides valuable demographic information about user who are seeing and clicking on your ads – key for optimizing your targeting filters."
- Actions by Impression Time: "This report shows the number of actions organised by the impression time of the Facebook Ad or Sponsored Story. An action is attributed to, categorized by the length of time between a user's view or click on the ad or sponsored story and the action taken (i.e., 0-24 hours, 1-7 days, 8-28 days)."
- Inline Interactions: "The Inline Interactions Report will help you understand the engagement on Page post ads. It includes metrics like impressions, clicks, and detailed actions such as likes, photo views, and view plays that happened directly from your ads."
- News Feed: "This report includes statistics about impressions, clicks, click-through rate (CTR) and average position of your ads and sponsored stories in news feed. Use it to analyse the performance of your ads and sponsored stories."

[37] Further documentation here: http://www.facebook.com/help/?page=198581376893307

Information about ad-clicks by Facebook users is stored in Hive and as such is subject to a table retention policy, as described in Section 1.9.2.2.1. The table retention policy for the two main ad-click tables in Hive has been reviewed and it has been confirmed that ad-click data will be de-identified after 90 days and deleted after 2 years. The content of the table has been examined and confirmed to be consistent with the retention policy.

2.4 Private Message Content

As part of this audit, Facebook were asked to provide information about what, if any scanning (aside from anti-virus and anti-spam scanning) is performed on user's private message content.

It has been reported in the media[38] that Facebook scan private messages in an attempt to identify child predators. Facebook have confirmed, as part of this audit, that scanning of a tiny fraction of private messages is taking place and have provided a description of the scanning process as follows; queries based on what FB-I describe as "objective non-content criteria determined to provide reasonable detection of a violation of certain terms of use of the service" identify a very tiny slice of sender-recipient pairs that match a specific profile. Stored messages matching that profile are ranked based on a specific list of keywords and a small number of the highest ranking conversations suggesting a possible risk of imminent harm are then queued for human review by a team of experts.

A full, detailed review of the operation of the private messaging system is beyond the scope of this audit.

2.5 Facebook Insights

When a website owner places a social plugin onto their web page, Facebook provide an interface through with aggregate information about the browsers that have interacted with that website can be viewed. This is known as Facebook Insights.

Similar functionality is available to Facebook page owners to view aggregate information about the interactions between Facebook users and the Facebook page.

FB-I report that non-Facebook user activity is currently represented in this information only as a count of interactions with the page or social plugin. The exact mechanism by which this aggregate information is calculated was not in-scope for this audit.

The functionality of Facebook Insights for social plugins and Facebook Insights for pages have been reviewed as part of this audit. It has been confirmed that all data presented to the website or page owner is aggregate and it is not possible to identify any information about individual user browsing patterns through this feature.

[38] http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

It has also been confirmed that if a Facebook user manages multiple Facebook pages there does not appear to be a way to cross-correlate the activity of one Facebook page with the activity of the second Facebook page within the Insights feature. Similarly, if a website owner adds social plugins to multiple websites, the aggregate information is presented separately for each social plugin and there does not appear to be a way to automatically cross-correlate the data relating to one social plugin with the data relating to the other social plugin within the Insights feature.

2.6 Page Uploads

It is possible for a Facebook page owner to upload a list of contacts and invite those contacts to visit and "like" their Facebook page. This is referred to as a page invite. Testing was performed to understand how this functionality operates and what the Facebook page owner can do with a list of uploaded contacts.

A page owner can upload a batch of email addresses (up to 5,000) and select which of the uploaded email addresses they want to send a page invite to. Obviously the imported list of email addresses can consist of various categories of email addresses;

- Email addresses of existing Facebook users
- Email addresses of non-users that had opted out of receiving communication from Facebook
- Email addresses of non-users that had not opted out of receiving communication from Facebook
- Email addresses at one of a list of blocked domains[39]

It was noted during this testing that before the Facebook page owner can submit the request to send emails to the list of imported contacts, they must confirm a checkbox that states "I am authorised to send invitations to the email addresses I've imported". If the page owner does not check this checkbox, it is not possible to send the emails.

FB-I report that the behaviour of the code is dependent on the geographic location of the page owner, as determined by the locale of the Facebook user. The testing performed as part of this audit took place within Ireland.

It was reported by FB-I that emails to non-users are silently dropped when the locale of the Facebook user (the page administrator attempting to send the page invites) is within the EU. Addresses mapping to Facebook users are delivered to the Facebook user's account.

[39] Facebook actively maintain a list of email domains that are popular exclusively within the EU and automatically block all page invite emails to those domains. Domains such as hotmail.com, yahoo.com and gmail.com that are popular globally are excluded from this list while domains such as yahoo.ie and other European-specific domains are included on the list.

It was not possible during the testing to cause page invites to be sent under any circumstances. Attempts were made to send page invite emails to:

- Existing Facebook users
- Non-users that had opted out of receiving communication from Facebook
- Non-users that had not opted out of receiving communication from Facebook
- A user at one of the blocked domains

None of the accounts ever received any page invite emails. FB-I report that if the administrator of the page who is attempting to send page invites is within the EU, all page invites will be silently dropped. Since the testing was performed from Ireland, the findings are consistent with this.

After the request to send the emails has been sent by Facebook, the list of imported data is not visible anywhere within the Facebook web interface. No record is retained of any contacts that were imported but not invited.

The fact that page invites have been sent to particular users is recorded as part of the underlying page owner's invitees, which are visible through that user's "Manage Invites and Imported Contacts".

The use of the "remove all your imported contacts" functionality works the same way as described in Section 1.1.1.

2.7 Deletion of National ID Data

Account authenticity issues can sometimes require users to submit identification to Facebook. For example, in cases where an account may have been compromised and none of the online remediation techniques succeed then the user can request access by submitting a ticket to FB-I's user operations.

This may require the user to send a copy of a piece of identification (such as a national identity card or passport) to FB-I. The picture of the identification is stored as an attachment to the user's ticket.

An automated process deletes attachments from tickets that have not been modified for 28 days. A review of the ticketing system was carried out during the audit and a selection of tickets were examined where the user would have been required to send identification to FB-I.

It was noted that all tickets examined that had not been modified for more than 30 days had no attachments remaining. This is consistent with the deletion of attachments by an automated process.

The code that performs the deletion of the attachments on tickets that have not been modified for more than 28 days was also reviewed and confirmed to operate as described here.

2.8 Deletion of Facial Recognition Data

Facebook have incorporated the ability of the site to build a "signature" of an individual's face based on photos in which they have been tagged. This allows Facebook to automatically suggest other photos in which a user's friend has not been tagged but may still be present.

It is possible that a user may want to disable this functionality and have the facial recognition data deleted.

A code review was performed to ensure that when a user disables the tag suggestions feature that the facial recognition data for that user is deleted. It has been confirmed that the AllFacesDataDeleter deleter from the deletion framework is run whenever the user chooses to disable tag suggestions. The behaviour of this deleter will be exactly as described in Section 1.9.2.1.

2.9 Record of Video Chat

The Facebook site has a video chat feature[40]. As part of this audit, FB-I were asked to report on what information they retain about the video chats that have taken place between users.

FB-I report that a record is maintained of the date and time of the most recent video chat between two users.

FB-I also note that data relating to the fact that a video chat has taken place is also stored in Hive but that this is not easily accessible as described in Section 2.1.

[40] https://www.facebook.com/videocalling/

Facebook Ireland Limited

Report to the Irish Data Protection Commissioner

July 2012

Table of Contents

APPENDIX

Chapter 1 – Facebook Ireland's Summary

This is a six-month follow-up report by Facebook Ireland (FB-I) in response to the recommendations made by the Office of the Irish Data Protection Commissioner (DPC) in its Report of Audit (December 2011) to FB-I with regard to FB-I's data protection practices and policies.

FB-I's report responds in sequential order to the recommendations made by the DPC in its Report of Audit by describing, and where appropriate providing screenshots of, the implementations of recommendations. Some such implementations may not be in final form, as of yet, but will be substantially similar to what is described or depicted in the screenshots. Where they are not in final form the schedule for implementation is listed.

FB-I has devoted considerable resources from nearly every part of the Facebook organization to fulfilling its commitments made during the audit last year. Literally hundreds of staff members and hundreds of thousands of hours have gone into making the numerous enhancements and improvements to FB-I's data protection and privacy practices, stucture, and policies.

FB-I has valued the on-going guidance and feedback received from the DPC, and has attempted always to achieve the result expected by the DPC. Inevitably, there have been differences in interpretation of the commitments, but in most cases, FB-I believes it has bridged the gap and fulfilled the DPC's expectations.

FB-I appreciates the acknowledgement by the DPC of the highly complex nature of its business, as well as its data storage and processing structure. FB-I believes it has gone above and beyond all comparable industry members in ensuring the most comprehensive data protection structure.

FB-I is proud of it accomplishments over the last six months and is grateful for the productive engagement with the DPC. We also recognise that the innovative nature of our business will require ongoing and close attention to our data protection obligations. We are devoting and will continue to devote the resources necessary to ensure that we fully meet those obligations.

Katherine M. Tassi
Head of Data Protection
Facebook Ireland

Chapter 2 – Privacy, Consent, Transparency, and Control

The DPC noted in the Report of Audit the challenges of conveying the complexities of the Facebook service, its data collection and use practices, the privacy controls, and product features to Facebook users. FB-I has made many substantial efforts to simpify all of these aspects of the service and platform. With more than 950 million active users ranging widely in age, language, country, education, etc., finding a communication model that is optimized for every user is extremely challenging. Nevertheless, FB-I constantly strives to do so. An important fact to bear in mind in evaluating how well FB-I does in communicating these important aspects of its service to users is that users respond differently from regulators and privacy advocates to web and social-networking experiences. There are certain communication norms that Facebook uses – accepted and expected ways of communicating things on the web, signals that communicate messages in shorthand for the quick-moving web-surfer. Whereas a regulator may believe a user would understand privacy better with a long, descriptive tutorial, FB-I's experience tells otherwise: the user is much more likely to surf away from that experience. The attention and interest span of web users is extremely short, their tolerance for long-winded disclosures and explanations is often quite low. Effective, realistic communication must be sensitive to these characteristics of web users. Therefore, FB-I strives for a balance and diversity in the ways it communicates important information to users. It uses words, symbols, icons, links, buttons, etc., and places such communications where the quick-moving web surfer's eyes are used to seeing such things. It is standard now to have links to privacy policies and terms of service above or below a button that people click to accept them. It is standard to have a "skip" link next to more prominent call-to-action buttons for optional steps in an online flow. FB-I's Data Use Policy represents one of its efforts to bring greater simplicity and accessibility to a privacy policy, which are typically extremely long, barely comprehensive documents written in legalese. FB-I's Data Use Policy, in the alternative, is simply written, contains visual illustrations, and is broken up into sections highlighted in a logical way. Another representative of FB-I's efforts to bring simplicity to its messaging to users is in the increased use of inline privacy settings with brief and targeted "tours" of how to use them.

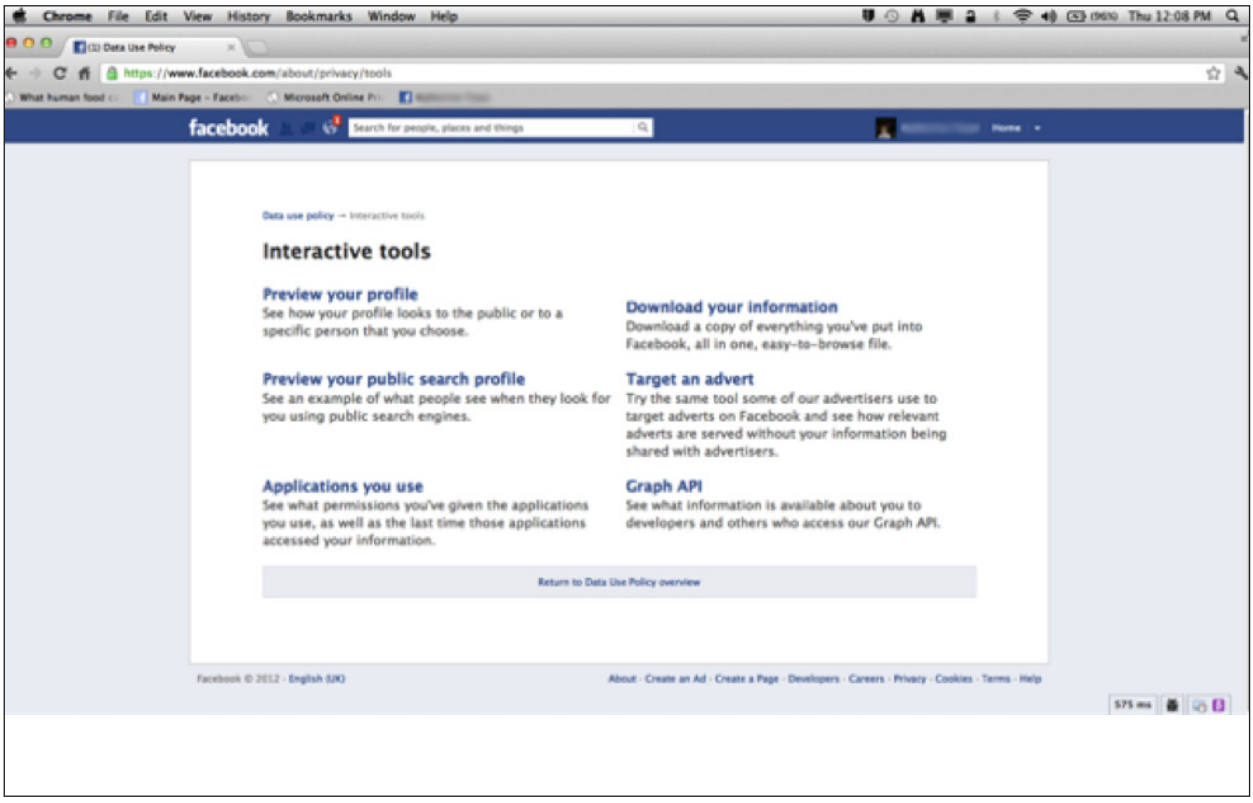
In giving effect to the DPC's recommendations throughout the Report of Audit, FB-I considered carefully how to give users meaningful notice, transparency, and control in the face of the reality of how web users behave and interact in the online world. FB-I wants users to understand its data practices, which are some of the best in the industry, and wants users to understand the product and services it offers, which come with unparalleled, granular controls. In giving effect to the DPC's recommendations, FB-I drew upon its seven years of experience in iterating and innovating its user interface, its messaging, its controls, its products, and, importantly, its users' feedback. See Appendix 1 (User Testing and Feedback).

2.1 Data Use Policy

European users consent to the collection and use of their personal data when they register for the Facebook service and are presented with FB-I's Data Use Policy and Statement of Rights and Responsibilities. FB-I's Data Use Policy comprehensively and clearly sets forth its policies on the collection and use of personal data it receives from users. The Data Use Policy is written in plain, easy-to-understand language, and includes many links to additional information, as well as visual depictions of certain aspects of the Facebook service. On the landing page for

the Data Use Policy, the content is presented under six headings, and additional resources are provided in prominent links on the right side of the page. See screenshot below:

The "Interactive tools" link takes users to a page with easy-to-read explanations of many useful features on Facebook, including how to access their personal data and where to view and control the applications they use. See screenshot below:



Most notably, in May 2012, FB-I proposed revisions to its Data Use Policy that substantially increased transparency in its data use practices by including more explanations, examples, and links to additional information. FB-I displayed prominent notice of the proposed revisions on users' homepages, as well as sent messages to all users who "like" the Facebook Site Governance Page. After the seven-day notice and comment period expired, FB-I considered all of the comments it received. FB-I addressed user comments by making some further revisions to the SRR reflecting user comments. For example, we rewrote Section 2.3 to clarify how sharing works with apps; rewrote Section 2.9 to clarify the proposed updates to our language on tagging; and removed our proposed addition of Section 17.4. Even where FB-I did not make revisions, FB-I provided further explanations of the original change. In fact, many of the user comments asked for explanations rather than for changes. Therefore. FB-I provided responses to the topics that sparked the most discussion. In light of the volume of comments received and as per FB-I's site governance policy, FB-I held a vote on the proposed revisions. FB-I adopted the revised policy on June 8, 2012.

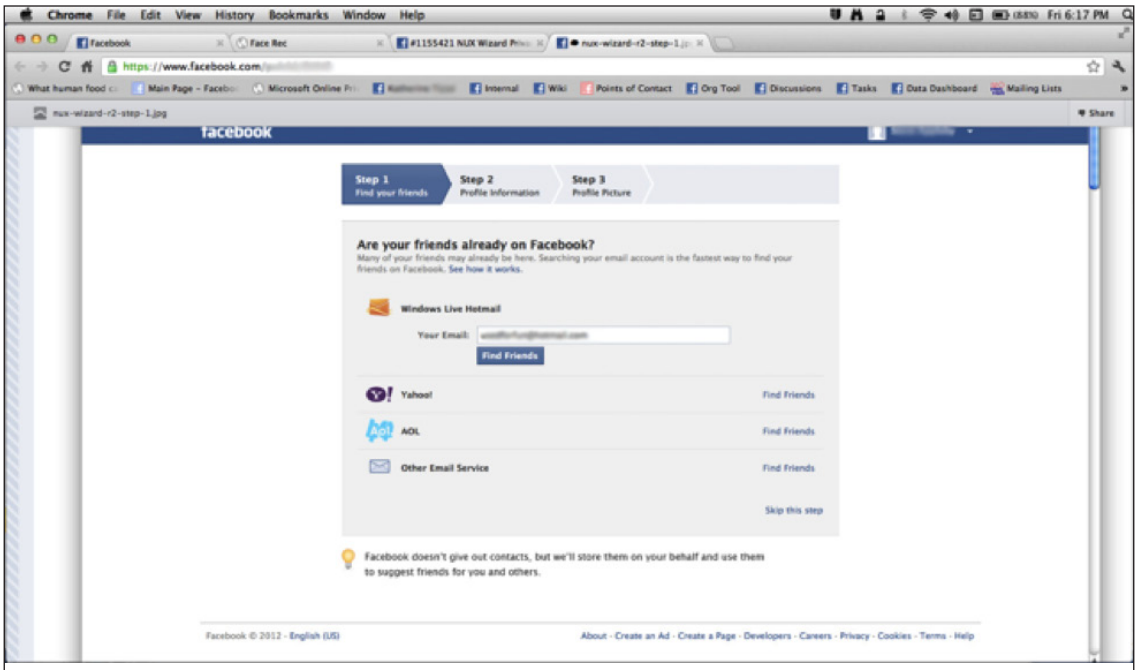
2.2 Registration Process

In response to the DPC's examination of new-user registration on Facebook and general recommendation that FB-I could make enhancements, FB-I changed the process in order to present the Data Use Policy and Statement of Rights and Responsibilites to users before they submitted any personal data. Previously, there was a two-step process, and the policies were not presented until after the user had completed the first step and submitted some initial personal data. FB-I has moved the links to the policies to the first step of the sign-up process, increased the size of the links, and has placed them more prominently above the sign-up button. FB-I also removed the words "and understand" in the agreement language at the specific request of the DPC. The DPC suggested that users would likely not be able to understand fully every aspect of the Data Use Policy before starting to use the Facebook service. See screenshot below:

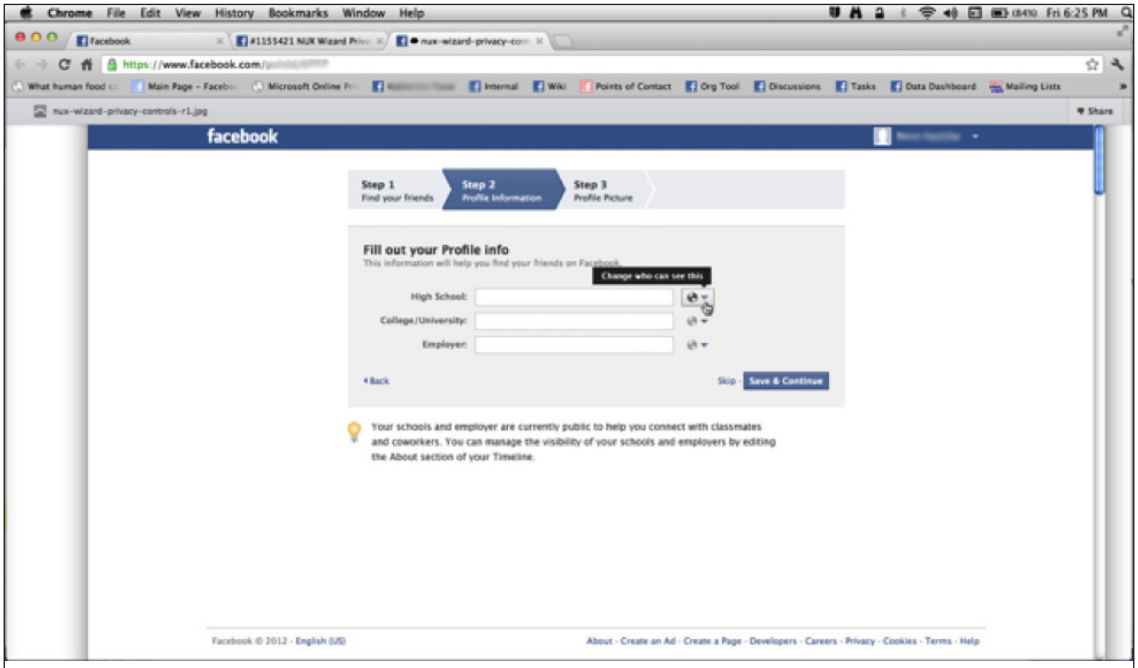
FB-I also added links to the Data Use Policy and Statement of Rights and Responsibilities, along with a link to our Cookies Use Statement, to the righthand side of the homepage of users; therefore, users have easy access to the policies directly from the homepage without having to scroll far down the screen. See screenshot below:

2.3 New User Experience

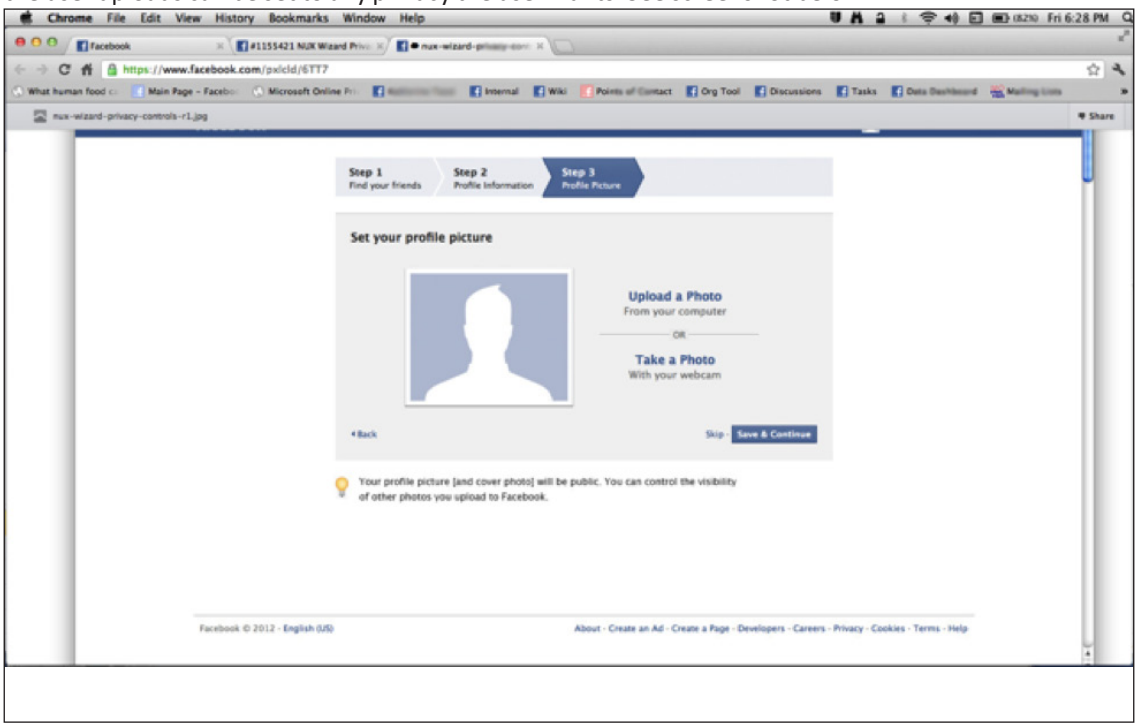
FB-I has also modified the screens that a new user sees when first joining the site so that relevant privacy information is highlighted contextually on each screen. The first screen a user sees after registering for an account prompts the user to find friends on Facebook by importing their contacts. FB-I added a prominent "lightbulb" icon at the bottom of the screen, providing users with information about how Facebook uses contacts and providing a link for users to learn more about the contact-importing process. See screenshot below:



The second screen prompts the user to fill in some initial profile fields – the schools they attended and their employer – information that increase the chances of the user finding friends more quickly. Because these fields are defaulted to public for adult users, FB-I has included a prominent lightbulb icon with the text informing the user why it defaults the fields to public and lets users know they can change the setting right there and then if they wish. FB-I also added a visibility-selector next to each of the fields so that users can change the setting right away. This also begins the process of assisting users to understand the meaning of the icons used for audiences on the site. See screenshot below:

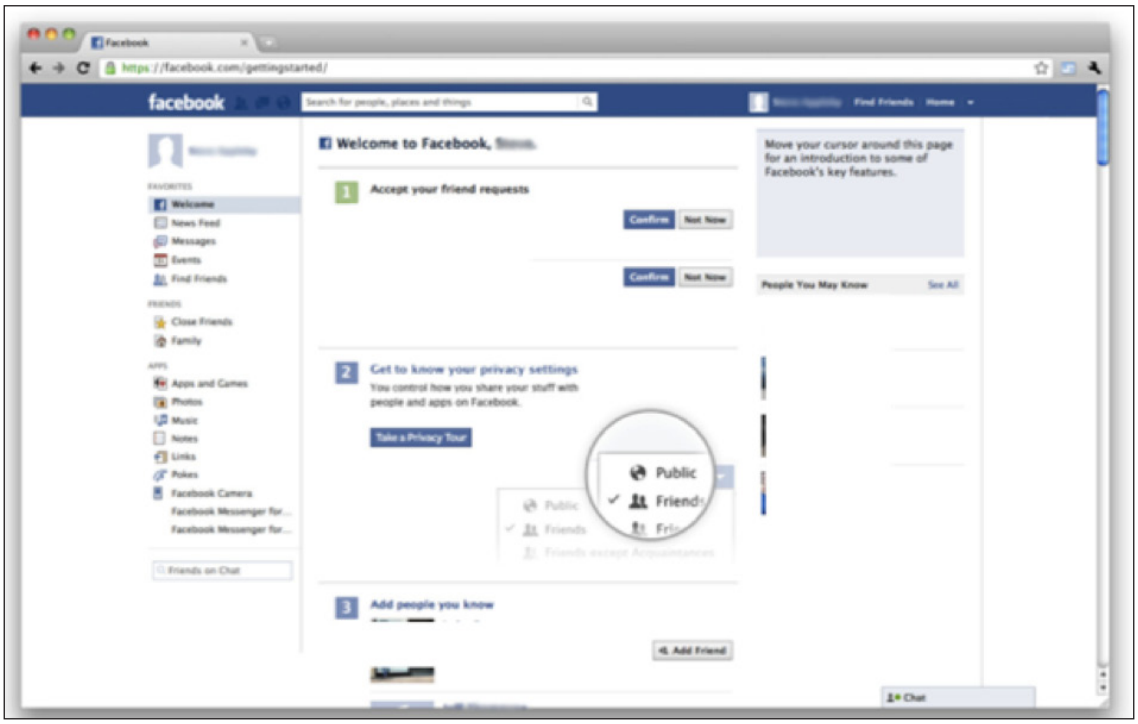


The third screen prompts the user to upload a profile photo. FB-I has included a prominent lightbulb icon with text informing users that the profile photo is public but that other photos the user uploads can be set to any privacy the user wants. See screenshot below:



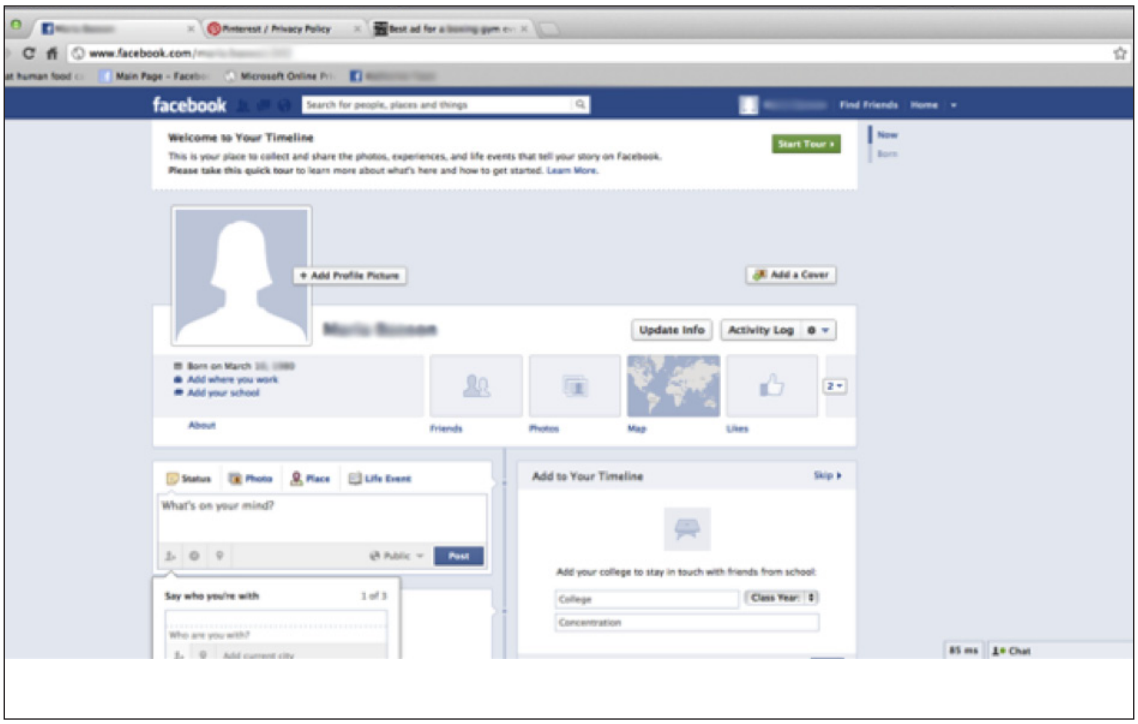
FB-I has tested two alternative additional steps for further new user education, which are described in section 2.6.

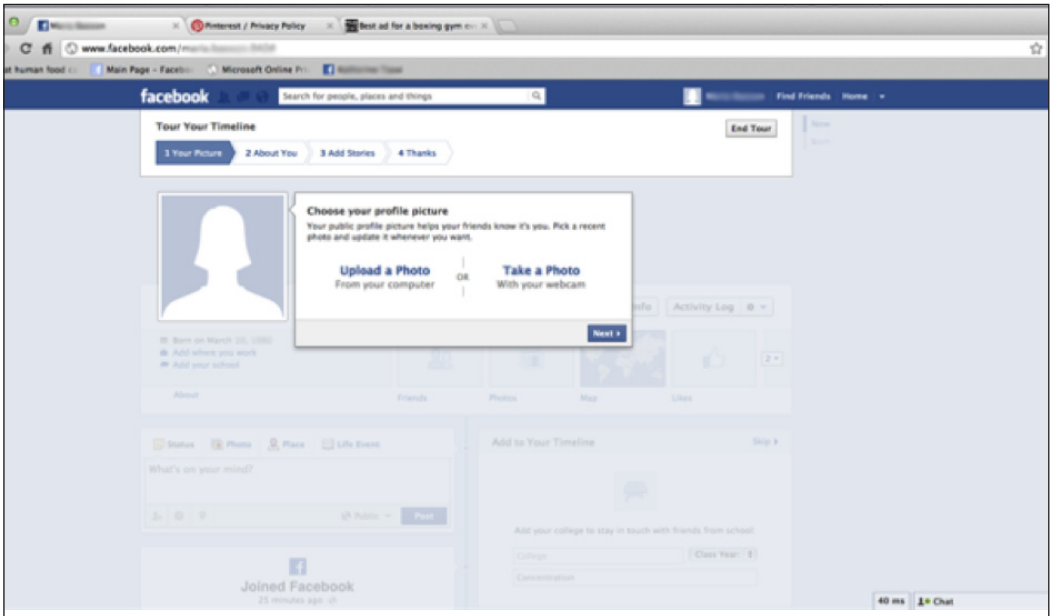
After uploading a photo, or skipping that step, the user lands on the “welcome dashboard”, which will provide a link for users to learn about their privacy settings. See screenshot below:

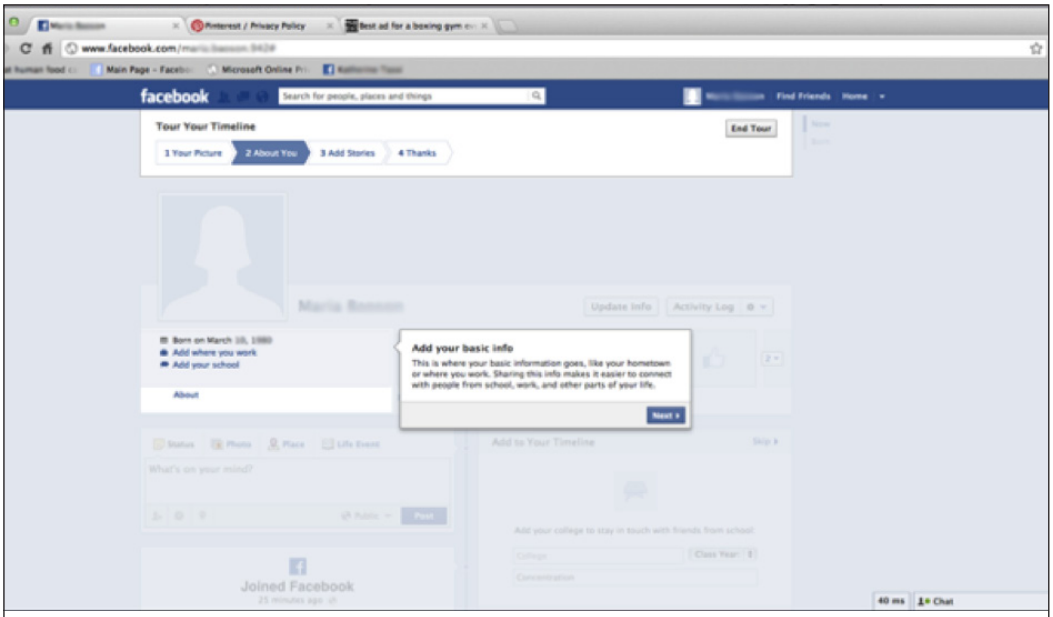


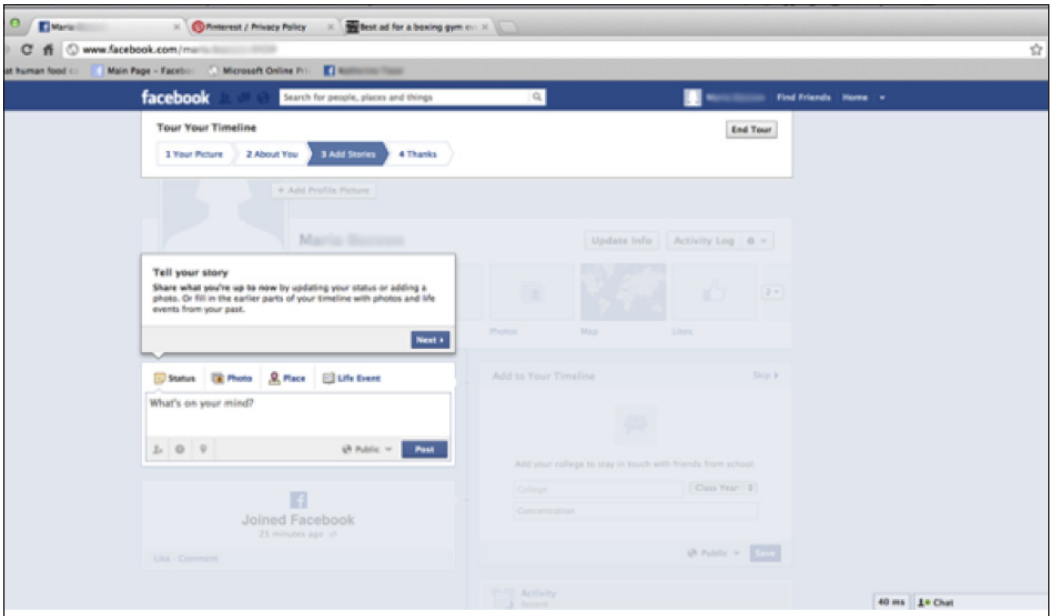
The link will pop up a modal, which will take the user through some key features of Facebook and the controls around them. See section 2.6 for screenshots

Finally, when a user finishes the initial steps of setting up their account, FB-I offers a short tour of timeline to help users navigate the features. This includes the status update tour discussed below. See screenshots below.




facebook
Tour Your Timeline
End Tour
1 Your Picture
2 About You
3 Add Stories
4 Thanks
Choose your profile picture
Your public profile picture helps your friends know it's you. Pick a recent photo and update it whenever you want.
Upload a Photo
From your computer
OR
Take a Photo
With your webcam
Next
Joined Facebook

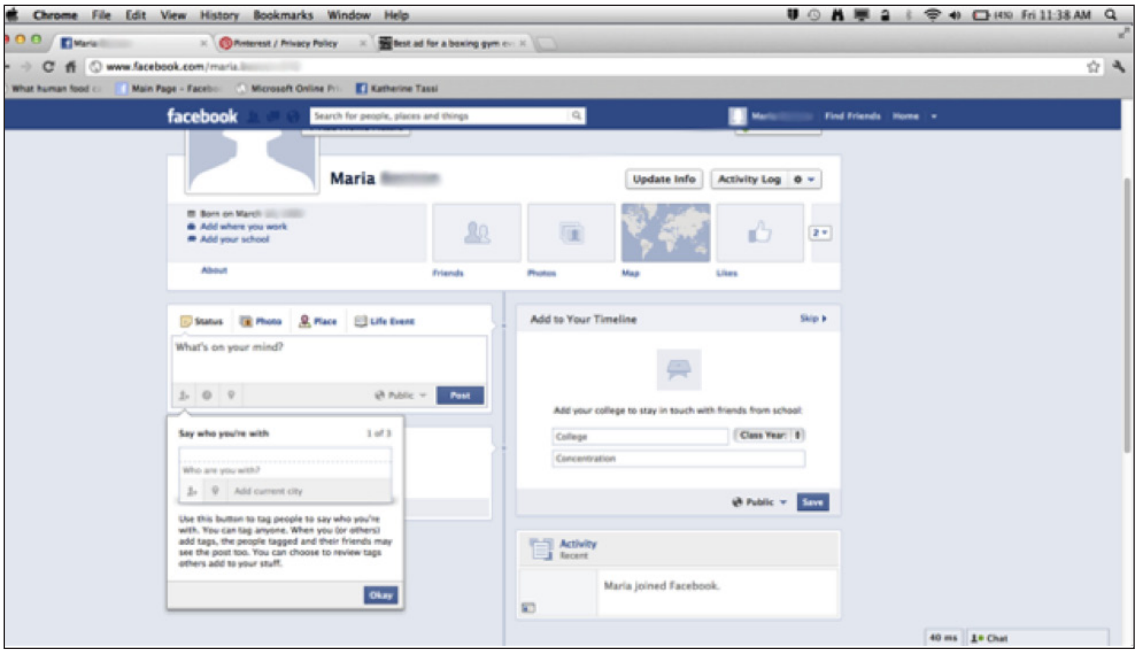

facebook
Tour Your Timeline
End Tour
1 Your Picture
2 About You
3 Add Stories
4 Thanks
Add your basic info
This is where your basic information goes, like your hometown or where you work. Sharing this info makes it easier to connect with people from school, work, and other parts of your life.
Next
About
Joined Facebook

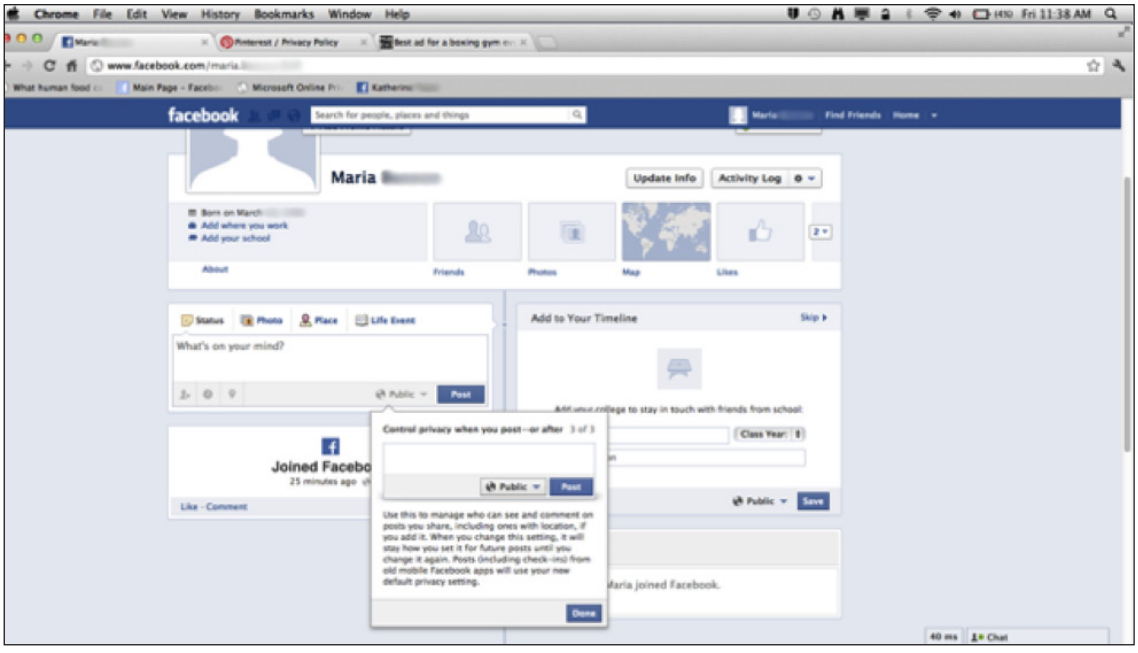

facebook
Tour Your Timeline
End Tour
1 Your Picture
2 About You
3 Add Stories
4 Thanks
Tell your story
Next
Status
Photo
Place
Life Event
What's on your mind?
Post
Joined Facebook

Along with new user education, FB-I is committed to providing education, contextual where appropriate, to users about new products and features, including reference to privacy and/ or visibility controls associated with the new product or feature, as well as periodically refresh users' knowledge of existing privacy and visibility controls through various means.

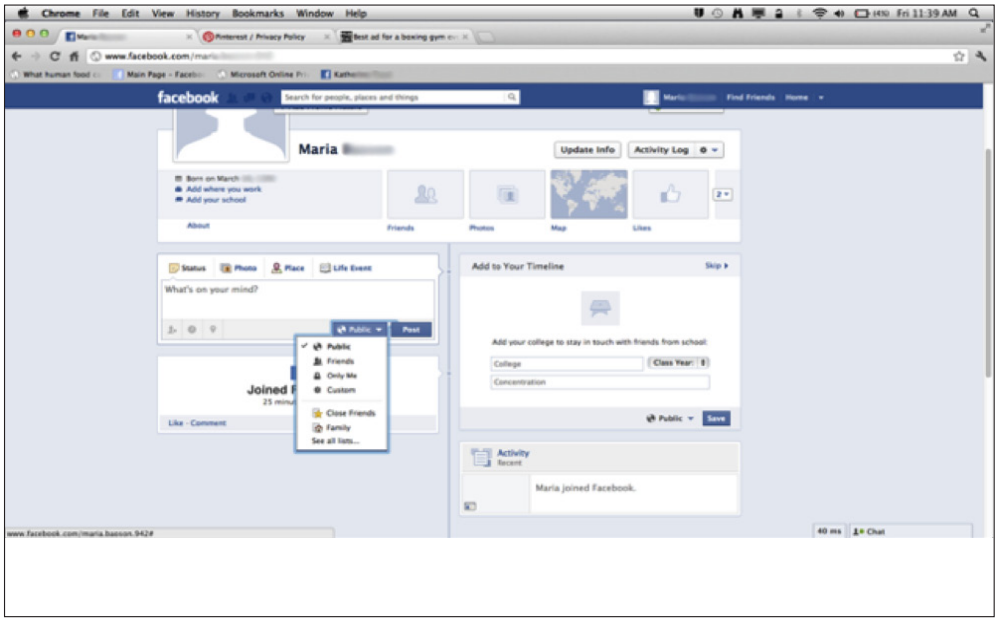
2.4 In-line Privacy Controls

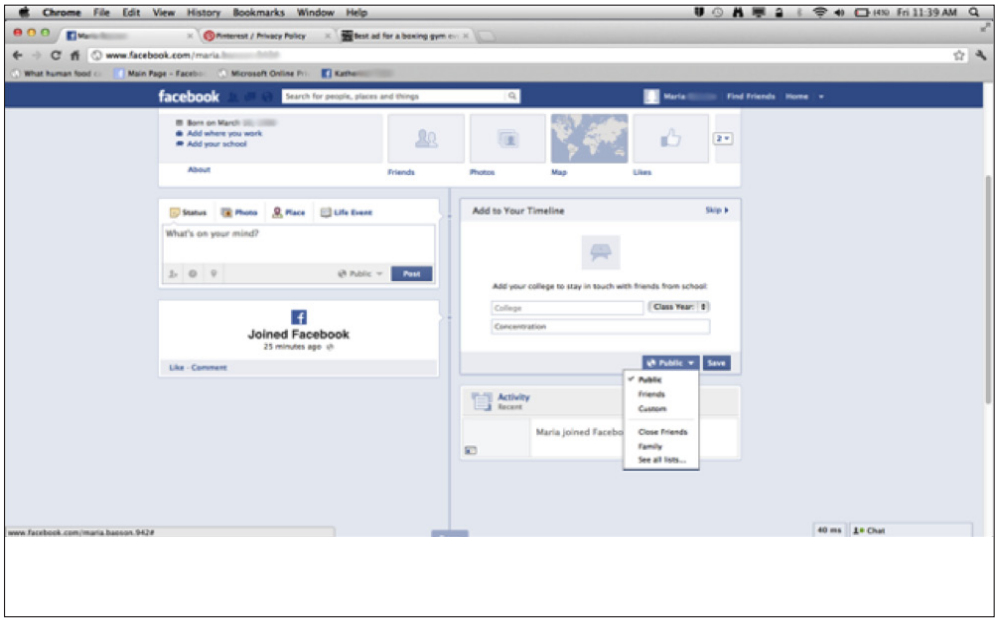
Facebook's privacy model has increasingly moved to one of inline, contextual control. FB-I has kept a minimum of settings that are not inline, and has moved most privacy settings to be contextual, beginning with the most important ones: status updates, which may contain text, location, photos, tags of people, places, or things, and shared information, like links to articles; and profile (timeline) information. The first time a user posts a status update, the user is given a tour of the settings and features in status updates, including the icons for the visibility options of public, friends of friends, friends, only me, and custom. See screenshots below:

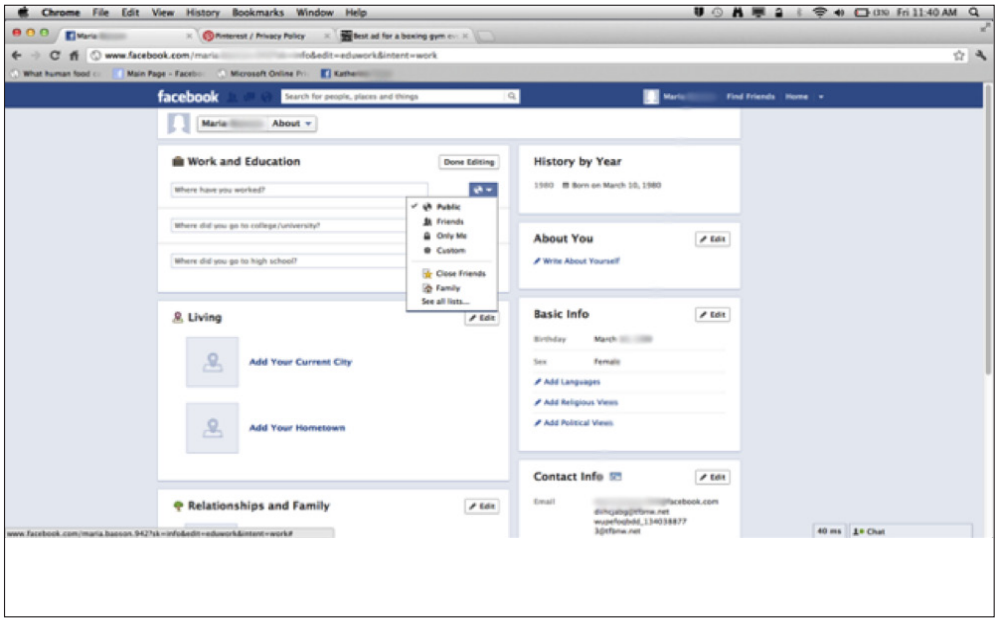


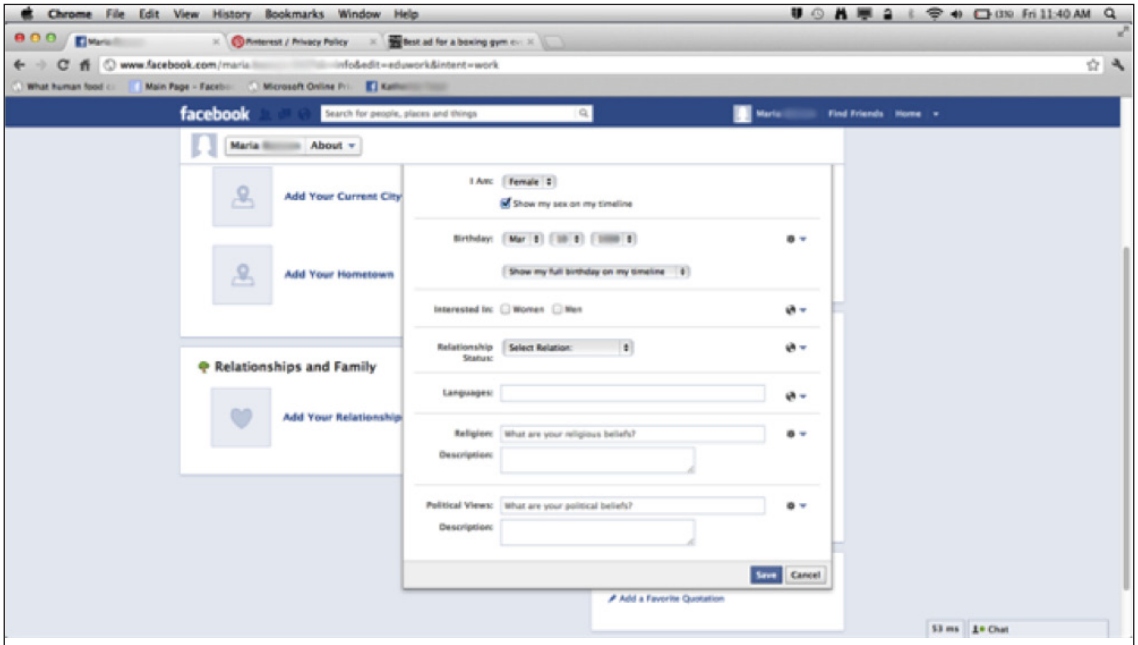


Second, FB-I added inline privacy settings for each field of information that a user can add to his or her profile. See screenshots below:

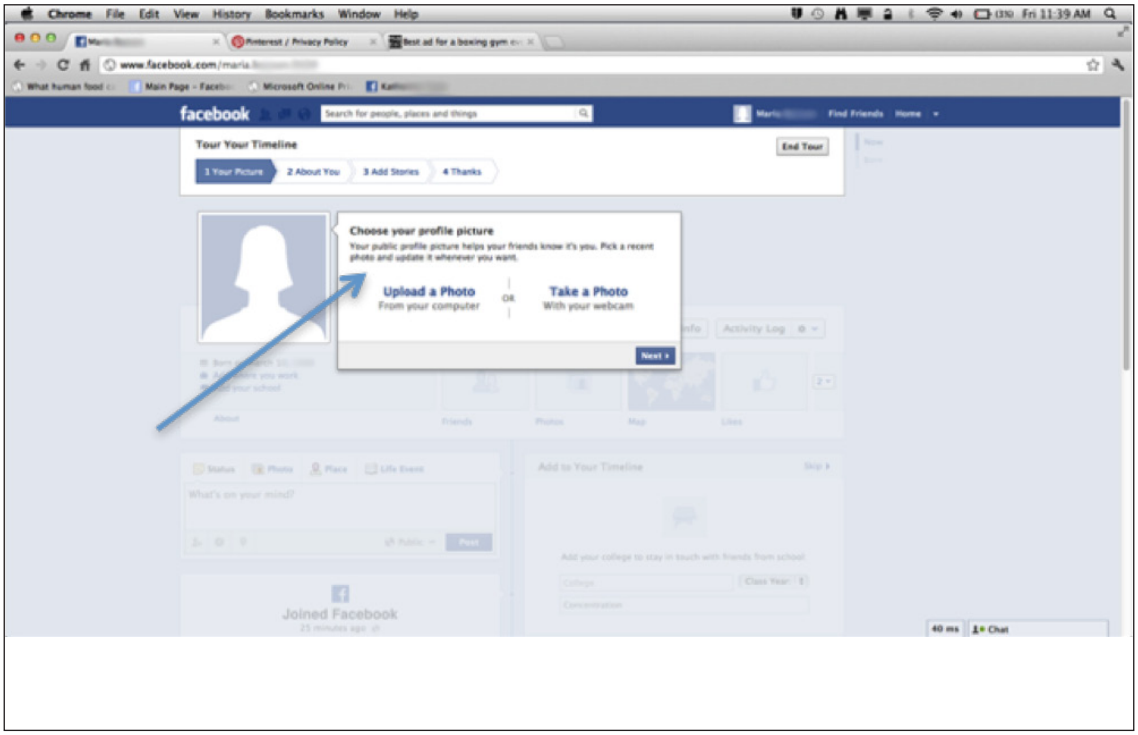






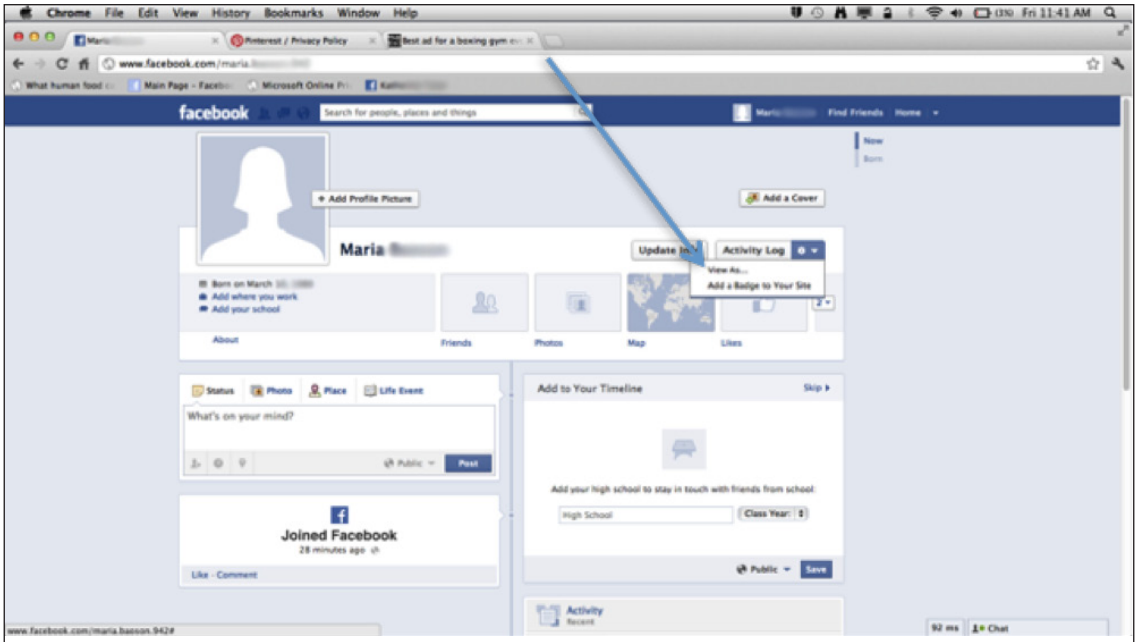


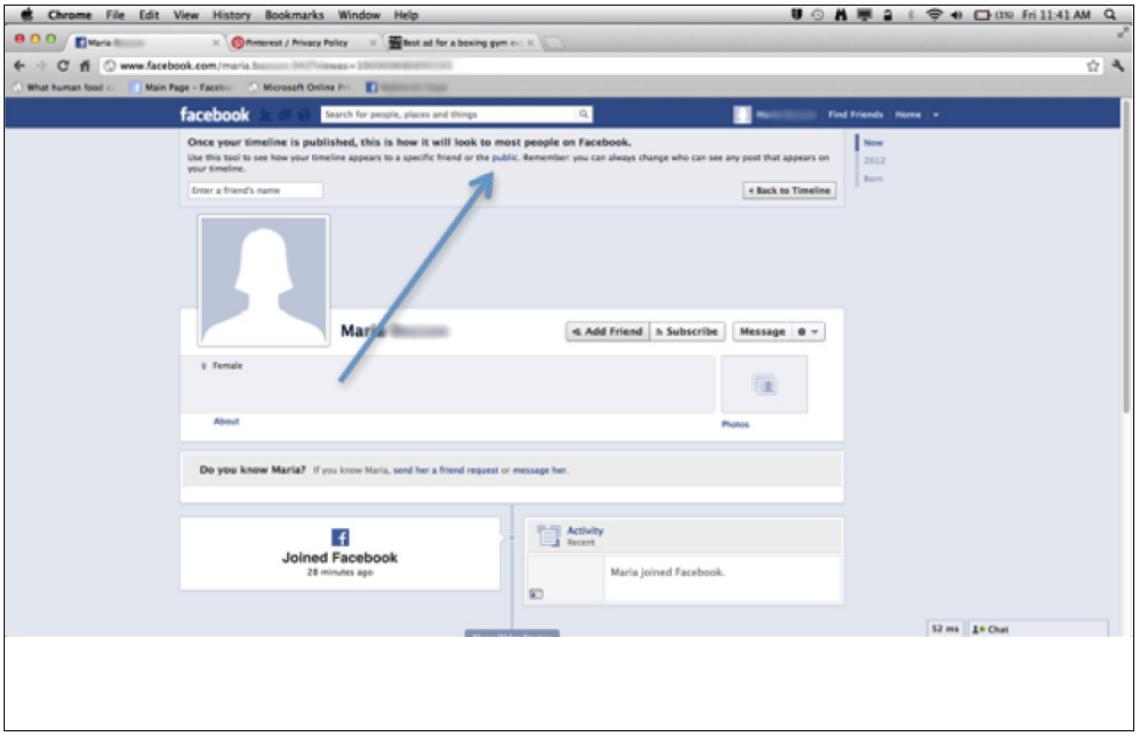
As well, if a user has not uploaded a profile photo during the new user experience but chooses to upload one later, FB-I added another reminder that the photo will be public. See screenshot below:



Another feature that FB-I offers new users is the ability to preview their timeline before they publish it. By using the "view as" control, users can test whether they have set the privacy controls as they wanted by viewing their timeline as if they were a stranger, or a specific friend. See screenshots below:

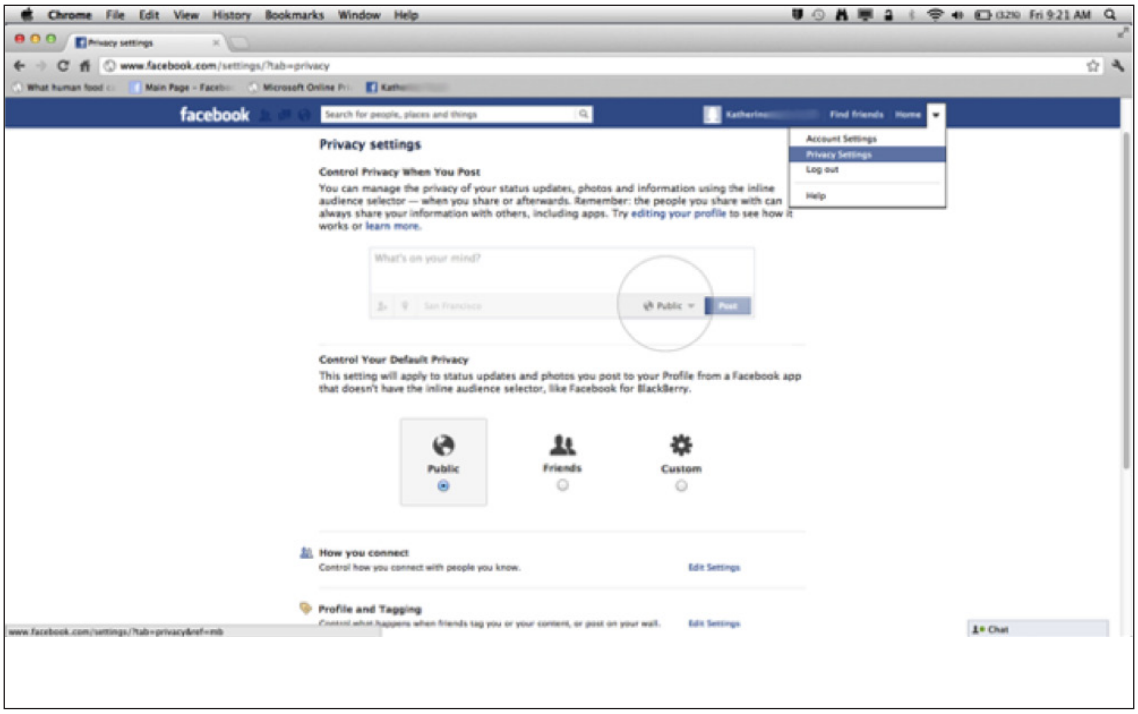
Another feature that FB-I offers new users is the ability to preview their timeline before they publish it. By using the “view as” control, users can test whether they have set the privacy controls as they wanted by viewing their timeline as if they were a stranger, or a specific friend. See screenshots below:



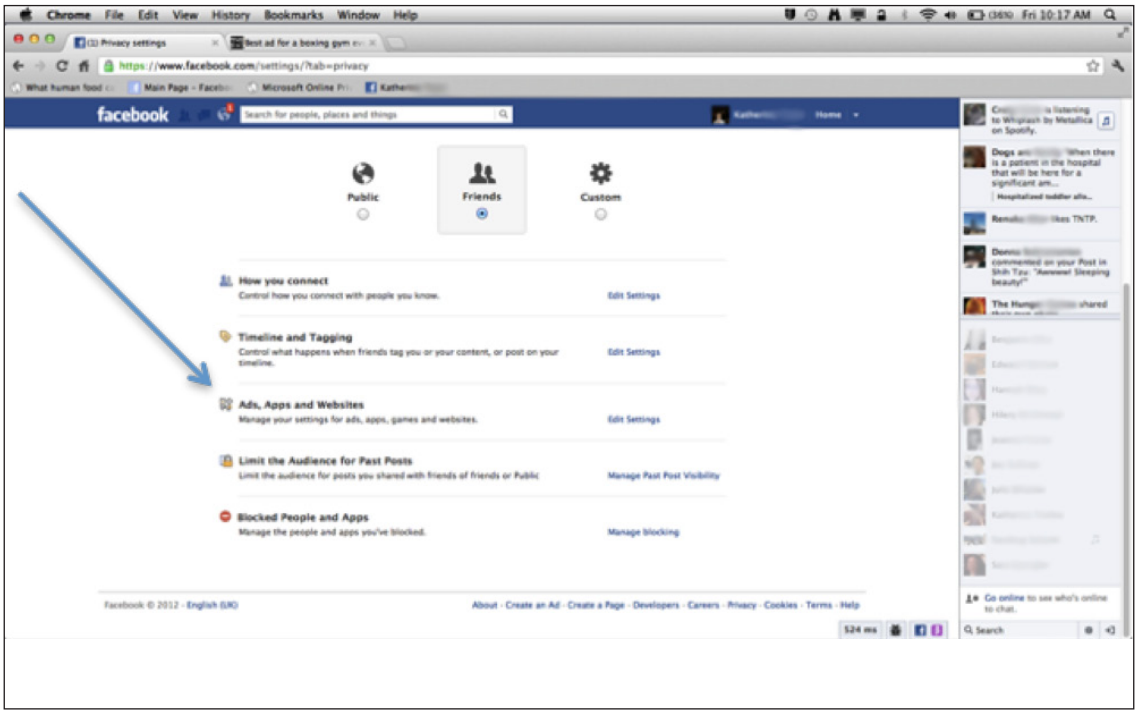


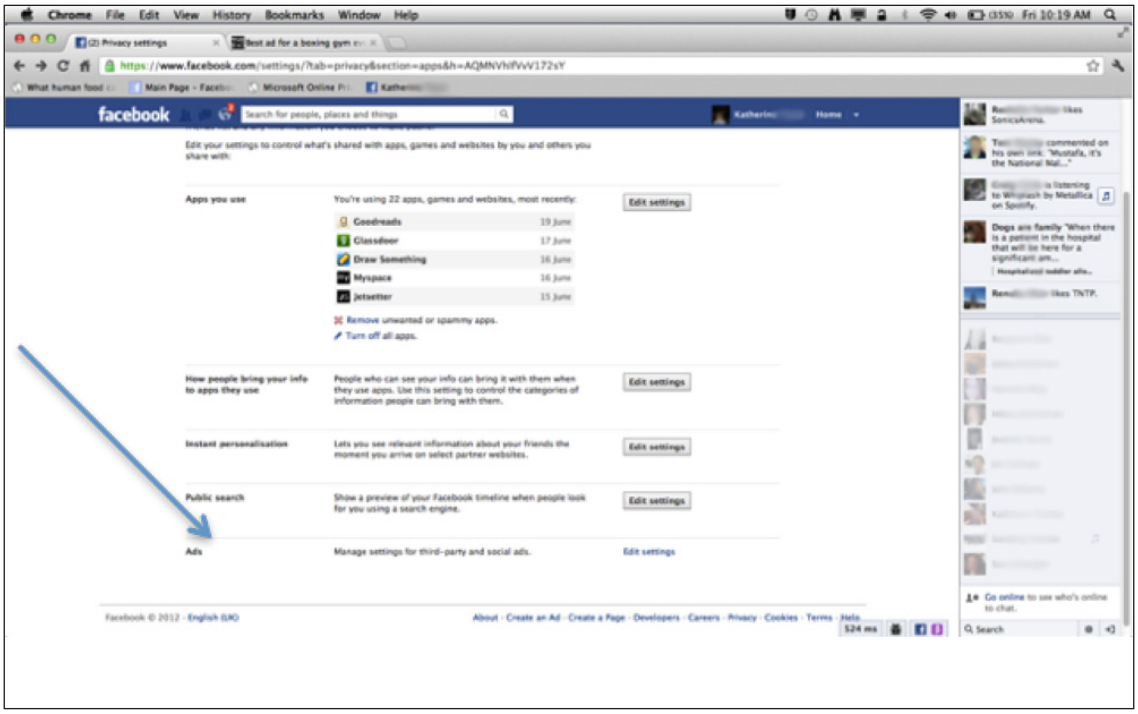
FB-I promotes the “view as” tool by showing a flyout on users’ timelines after the user has been on the site for up to 30 days. See screenshot below.

In addition, a user’s privacy settings are easily accessible through a link in the top righthand corner of every page. See screenshot below:



Further, in response to the DPC's recommendation that the settings related to ads be accessible from the privacy settings rather than the account settings, FB-I moved the ads settings to the privacy settings. See screenshots below

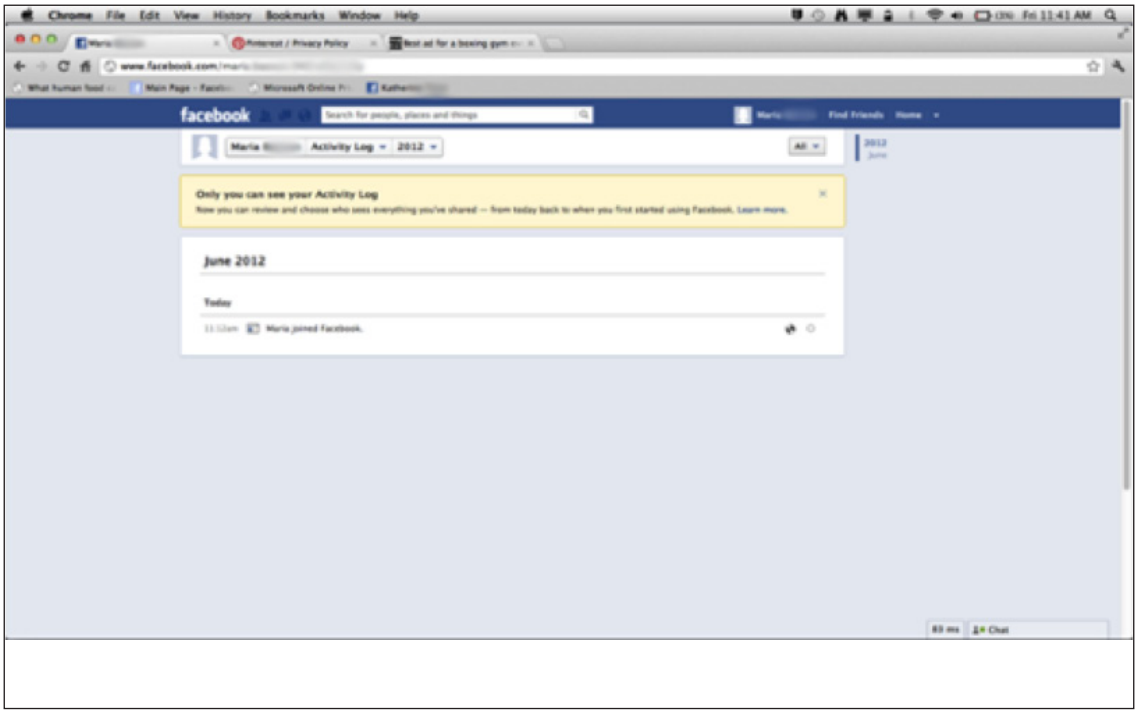




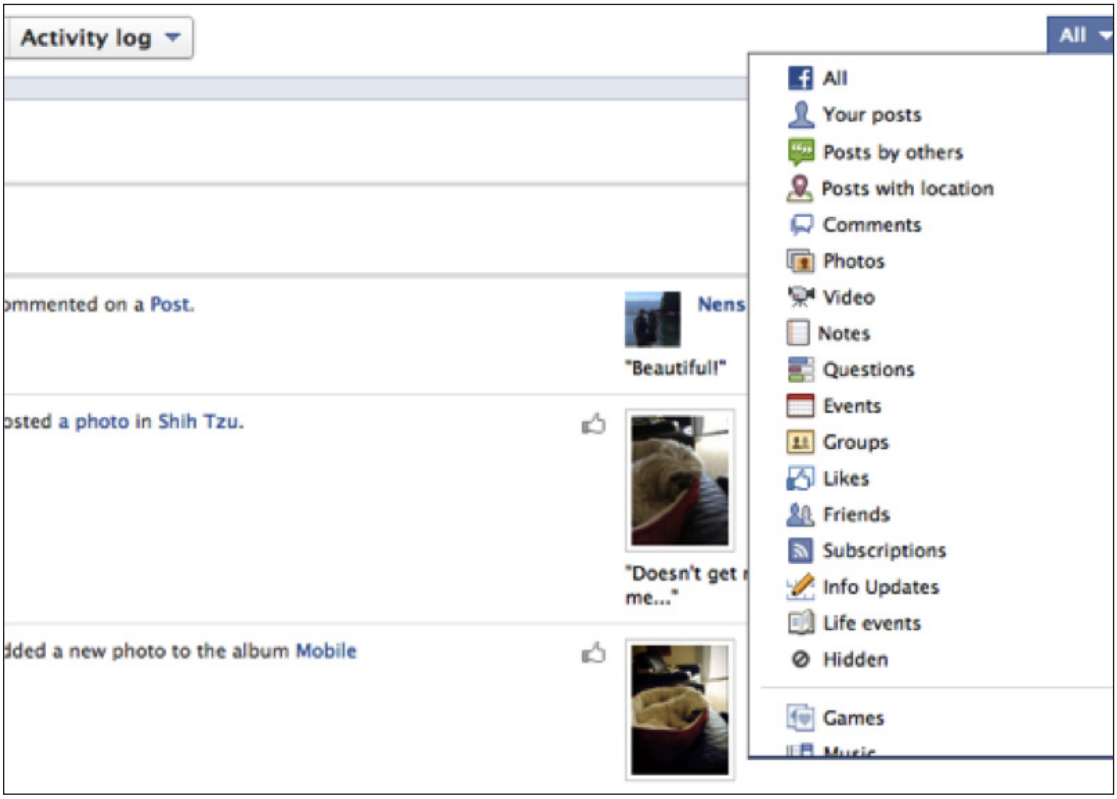
(note: "edit settings" link will be changed to a button)

2.5 Transparency and Control

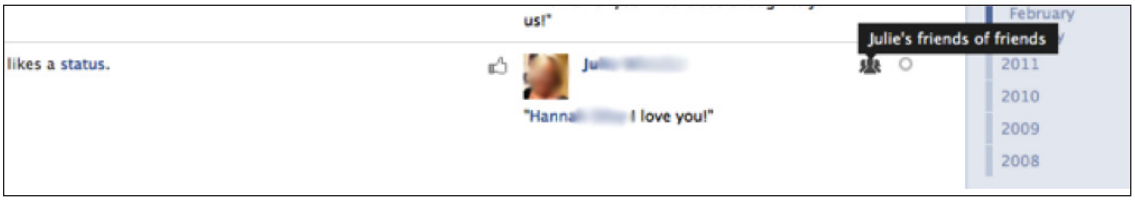
The transparency and control offered by Facebook's Activity Log feature is a major accomplishment. This is one of the most innovative and unparalled offerings in the social media industry and clearly demonstrates FB-I's commitment to integrating transparency and control over data into the Facebook experience. This feature was introduced prior to the audit, but has been further developed and elaborated over the past six months in response to the audit, including adding the feature to the profiles of users who still have not transitioned to timeline. Activity Log, which is visible only to the user herself, presents users with a detailed and comprehensive look at all of their activity on Facebook since the beginning of their accounts. Users can sort by activity type, e.g., "comments", "status updates", "likes", or can search the Activity Log using keywords. Users can also jump to any month and year to view the activity during that time period. Further, the Activity Log provides users the ability to see in one place the visibility setting of their activity and the objects they interacted with, as well as the ability to change the visibility, remove from timeline, or delete the activity. The Activity Log shows whether a user added location to a post and whether the post received comments. The Activity Log is extremely easy and intuitive to navigate – a user need only hover with his cursor over any part of the log to learn what it means. See screenshots below:



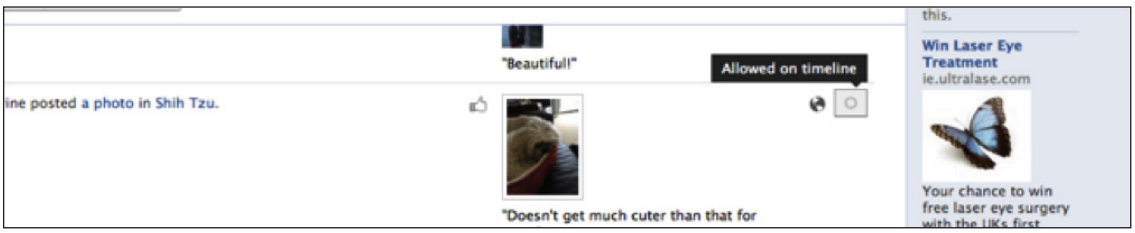
(new user's first time in Activity Log)



(Sort by activity)



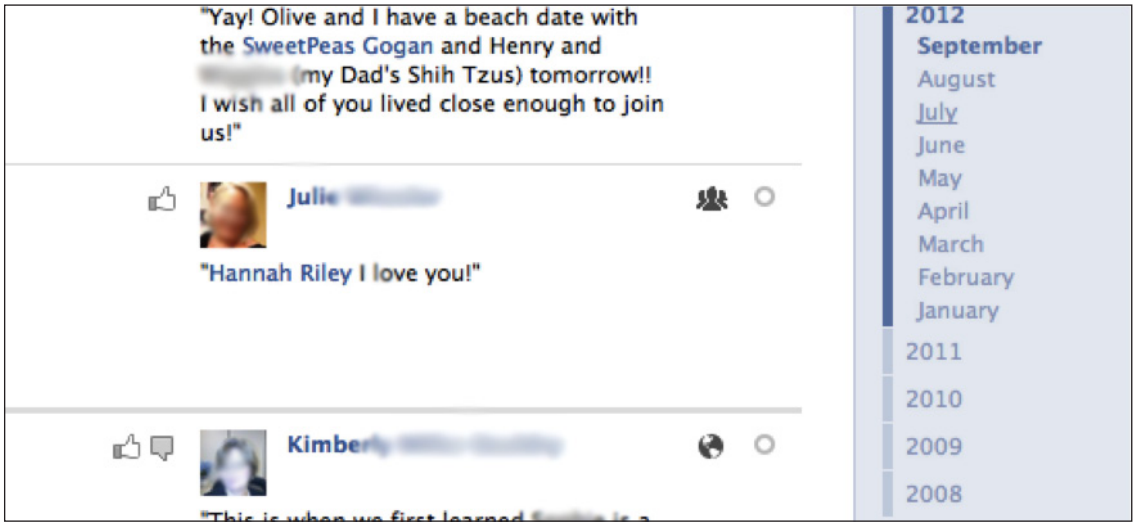
(Visibility of third-party object user liked)



(whether action appears on user's timeline)

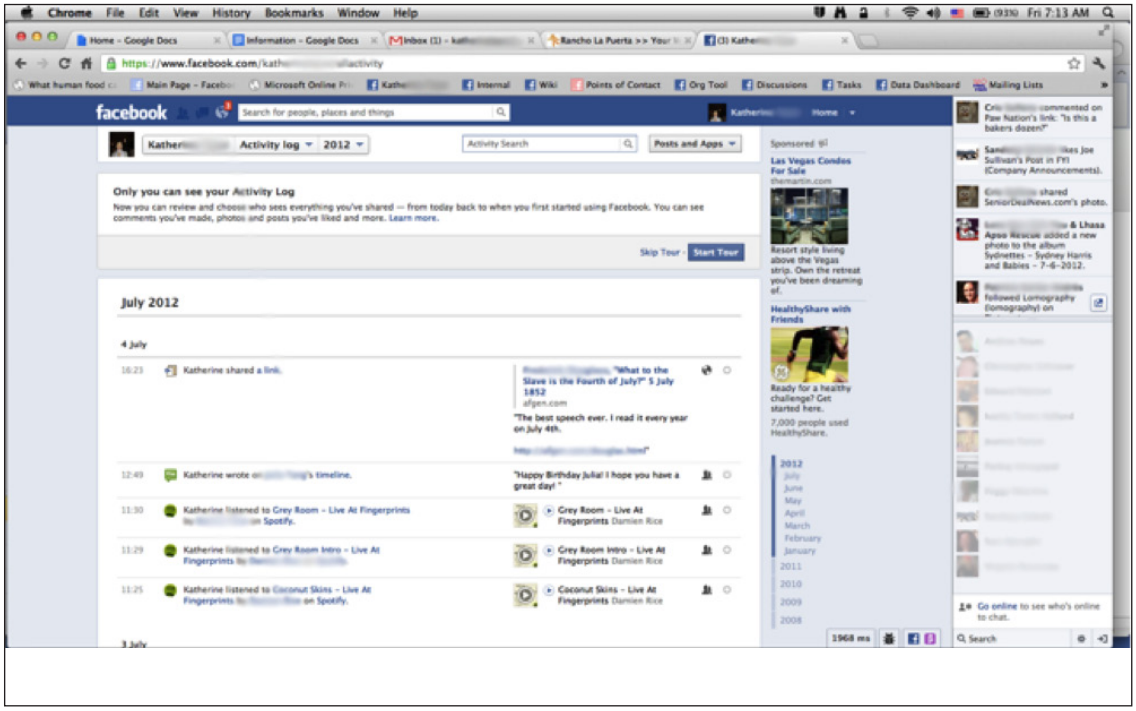
(whether there are any comments on the third-party object)

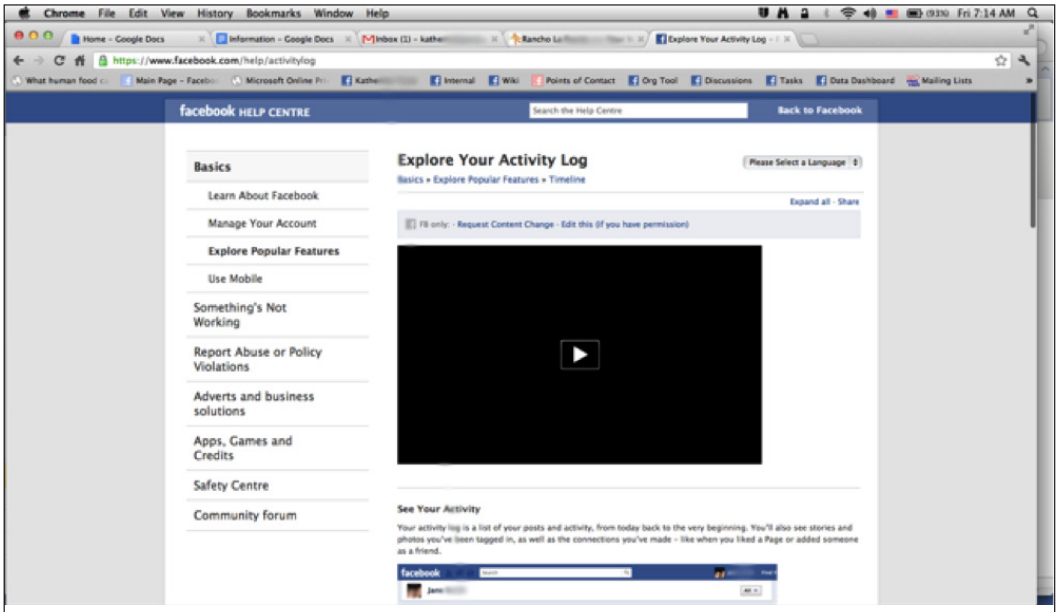
(location, if added)

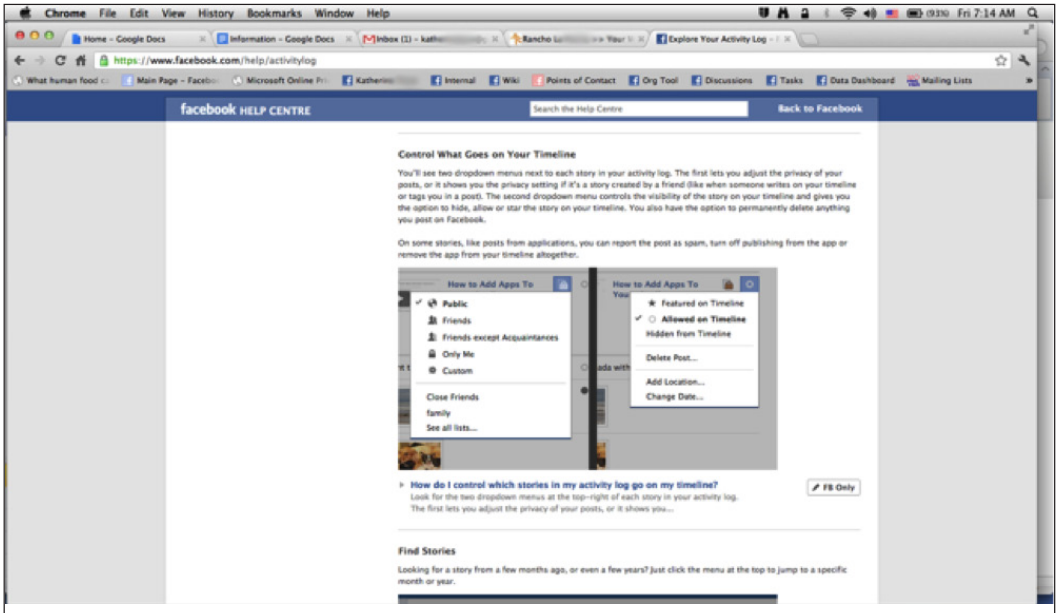


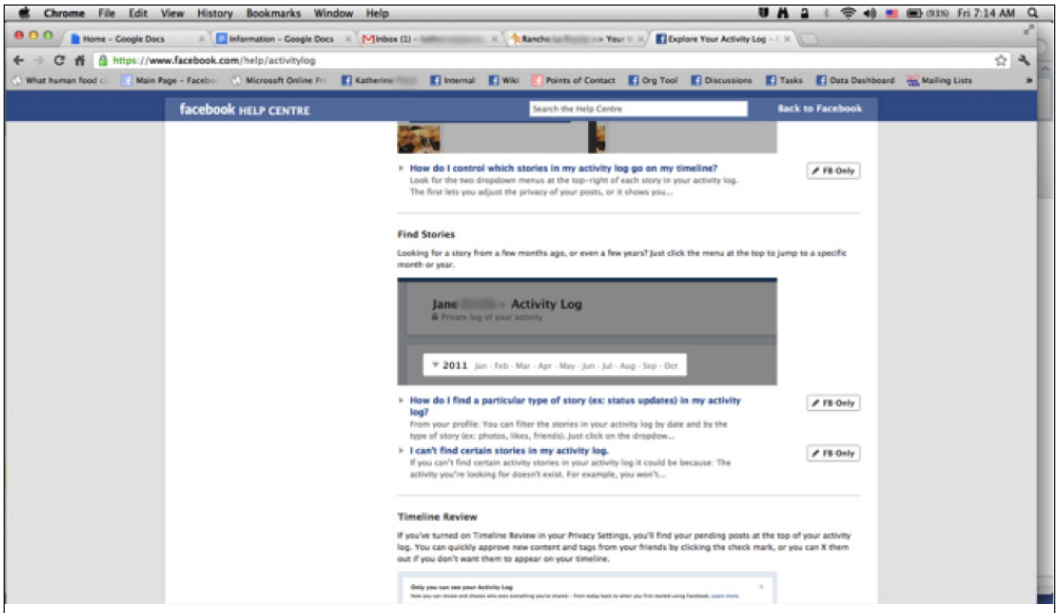
(can easily jump to a period earlier in time)

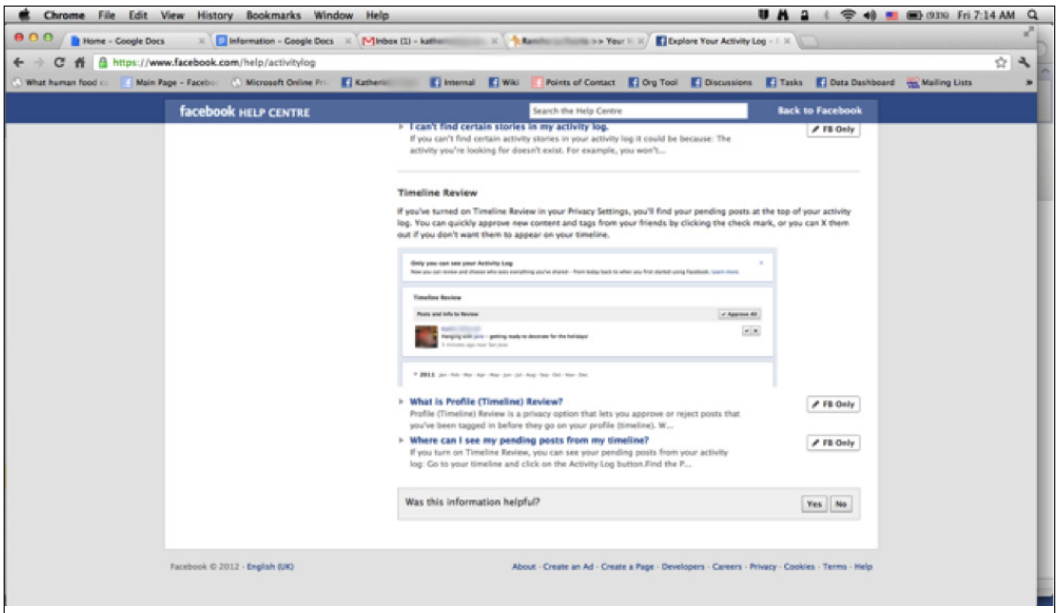
Additionally, users who first visit the Activity Log are provided an Activity Log educational tour. See screenshots below.




facebook HELP CENTRE
Search the Help Centre
Back to Facebook
Basics
Learn About Facebook
Manage Your Account
Explore Popular Features
Use Mobile
Something's Not Working
Report Abuse or Policy Violations
Adverts and business solutions
Apps, Games and Credits
Safety Centre
Community forum
Explore Your Activity Log
Please Select a Language
Basics » Explore Popular Features » Timeline
Expand all · Share
See Your Activity


facebook HELP CENTRE
Search the Help Centre
Back to Facebook
Control What Goes on Your Timeline
How to Add Apps To
Public
Friends
Friends except Acquaintances
Only Me
Custom
Close Friends
family
See all lists...
Featured on Timeline
Allowed on Timeline
Hidden from Timeline
Delete Post...
Add Location...
Change Date...
How do I control which stories in my activity log go on my timeline?
FB Only
Find Stories

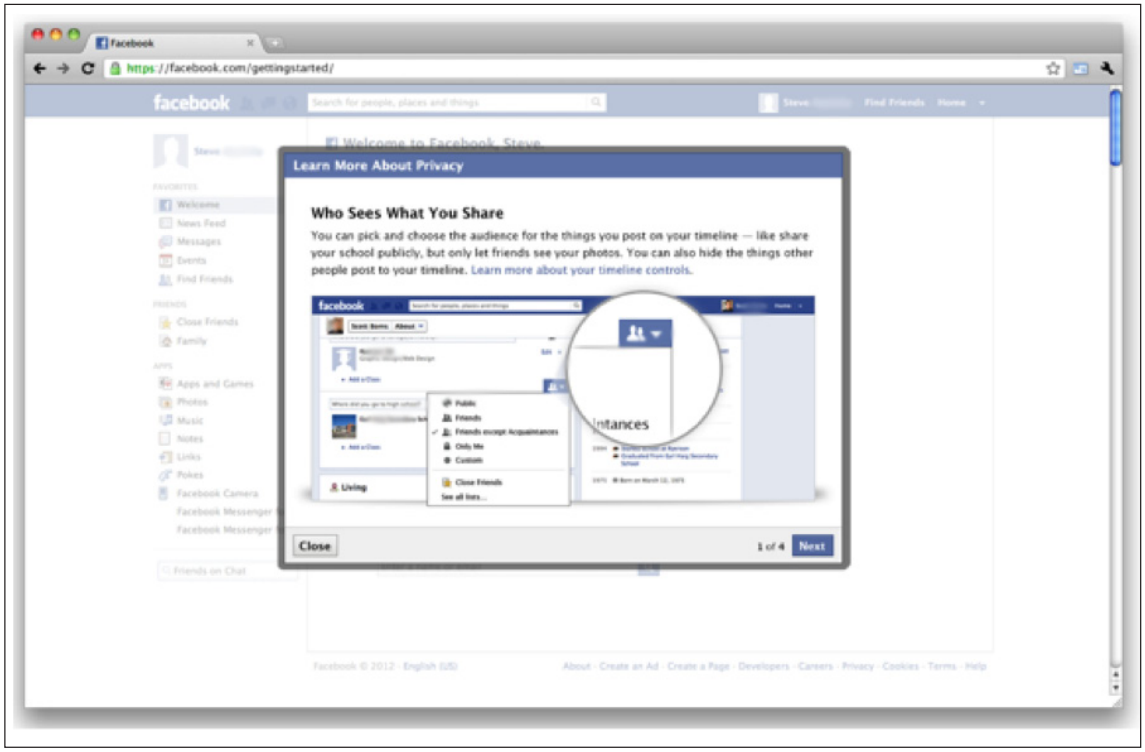

facebook HELP CENTRE
Search the Help Centre
Back to Facebook
How do I control which stories in my activity log go on my timeline?
FB Only
Find Stories
Activity Log
2011
How do I find a particular type of story (ex: status updates) in my activity log?
I can't find certain stories in my activity log.
Timeline Review

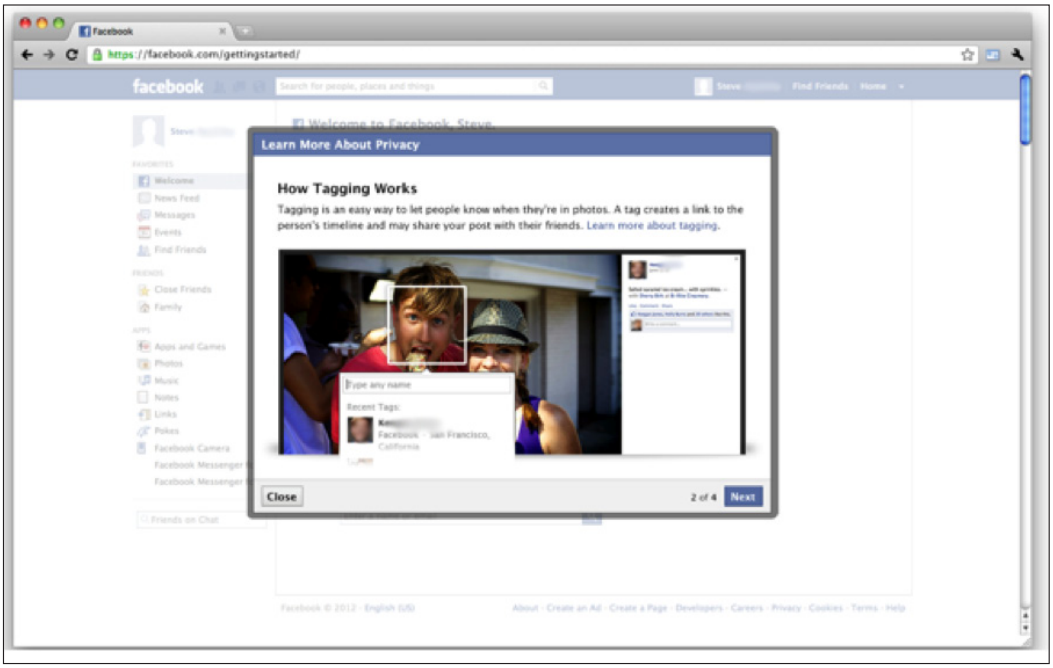

Chrome File Edit View History Bookmarks Window Help
https://www.facebook.com/help/activitylog
facebook HELP CENTRE
Search the Help Centre
Back to Facebook
I can't find certain stories in my activity log.
FB Only
Timeline Review
If you've turned on Timeline Review in your Privacy Settings, you'll find your pending posts at the top of your activity log. You can quickly approve new content and tags from your friends by clicking the check mark, or you can X them out if you don't want them to appear on your timeline.
What is Profile (Timeline) Review?
FB Only
Where can I see my pending posts from my timeline?
FB Only
Was this information helpful?
Yes
No
Facebook © 2012 · English (UK)
About · Create an Ad · Create a Page · Developers · Careers · Privacy · Cookies · Terms · Help

2.6 New User Privacy Education

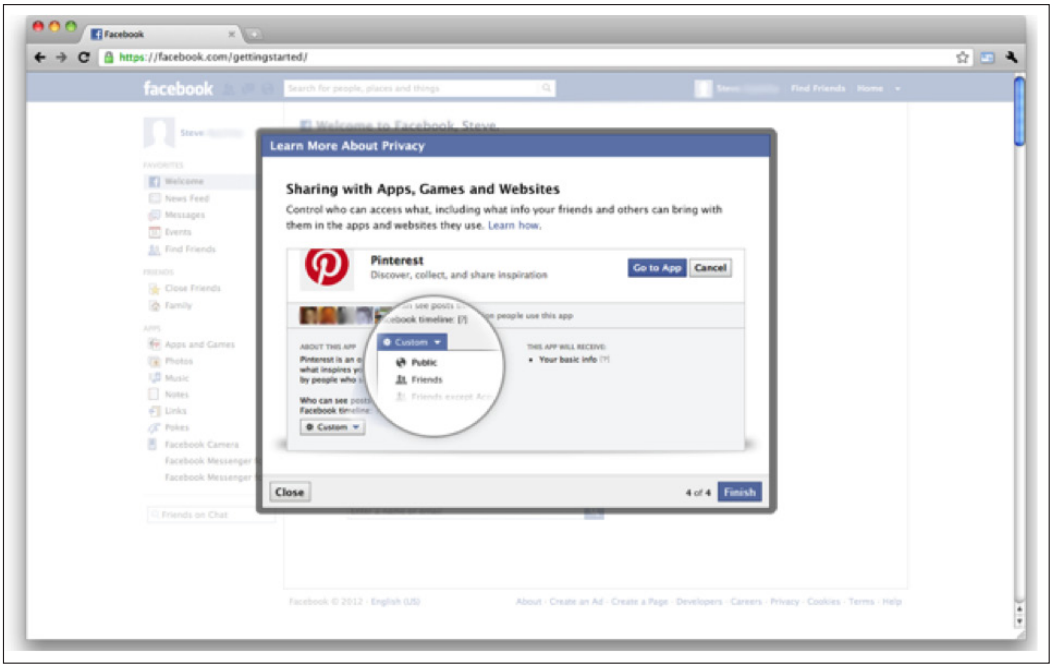
The DPC recommended that FB-I evaluate the totality of its guidance to new users about privacy features. In doing so, FB-I made the enhancements described above, but also Expanded new user privacy education by introducing resources available to users to learn more about various aspects of the Facebook service and platform and the controls available to users. On the "welcome dashboard", which is the page new users land on after going through the three steps shown above in section 2.3, the user is introduced to some of the key features and privacy controls on Facebook. See screenshot below:

By clicking on "Take a Privacy Tour", the user is introduced to the core parts of the Facebook service via a four-step modal: (1) Who Sees What You Share, (2) How Tagging Works, (3) How You Connect With Friends, and (4) Sharing With Apps, Websites, and Games. See screenshots below:




Facebook
https://facebook.com/gettingstarted/
facebook
Learn More About Privacy
How Tagging Works
Tagging is an easy way to let people know when they're in photos. A tag creates a link to the person's timeline and may share your post with their friends. Learn more about tagging.
Close
2 of 4
Next


Facebook
https://facebook.com/gettingstarted/
facebook
Learn More About Privacy
How You Connect with Friends
You can control who can send you friend requests in your How You Connect settings.
Everyone
Done
Close
3 of 4
Next


Facebook
https://facebook.com/gettingstarted/
facebook
Learn More About Privacy
Sharing with Apps, Games and Websites
Control who can access what, including what info your friends and others can bring with them in the apps and websites they use. Learn how.
Pinterest
Discover, collect, and share inspiration
Go to App
Cancel
Public
Friends
Close
4 of 4
Finish

Each of these sections contains a link to a page on Facebook that provides detailed information about that feature, including links to the privacy controls associated with the feature. See

https://www.facebook.com/about/sharing, https://www.facebook.com/about/timeline,

https://www.facebook.com/about/tagging, https://www.facebook.com/about/platform.

Chapter 3 – Advertising

The DPC in its Report of Audit described advertising on Facebook as its principal Facebook later gives this nickname back to the partner when soliciting advertising bid requests. source of revenue. The Report noted that FB-I targets ads using some of the data about users that it receives. As the Report observed (at 5), "FB-I provides a service that is free to the user. Its business model is based on charging advertisers to deliver advertisements which are targeted on the specific interests disclosed by users. This basic 'deal' is acknowledged by the user when s/he signs up to FB-I and agrees to the Statement of Rights and Responsibilities and the related Data Use Policy."

Indeed, advertising is critical to FB-I's business, and targeting ads based on data we receive from or about users creates FB-I's value to advertisers and aims to give users more relevant and useful ads. FB-I has a commitment, however, not to sell users' personal data to advertisers or other third parties nor share any personal data (without the user's permission).

It is essential to FB-I's continued success as a business that it develop and innovate in both its user-facing products and its advertiser-facing products. FB-I must improve the return on investment for advertisers in order to continue to thrive as a business and provide users with the services they want for free. Staying the same is not an option.

However, FB-I, as it offers new options to advertisers, very carefully evaluates and analyzes the impact on, and benefits to, users of expanding the variety of data that is used to target ads.

3.1 Social Plugin Impression Data

The Report of Audit confirmed that (a) FB-I did not use the data it received when logged-in users visited sites with social plugins for advertising purposes, and (b) FB-I only used such data for the purposes of bug-fixing and analysis of social plugin performance.

3.2 Keywords and Search Terms

FB-I discloses in its Data Use Policy that it may use any data it receives to target ads. There are some limitations, however, and FB-I understands that certain forms of advertising may call for enhanced notice and consent. In response to the recommendation of the DPC that it give users better notice that it may use keywords from status updates to inform its ad-targeting, FB-I included further information about this use of data in its revised Data Use Policy. Further, FB-I recently launched "sponsored search results", where an advertiser can bid on a keyword when a user searches for a particular Page, product, company, etc. For example, if a user types in "coffee" in the search box, we might show a sponsored result for the Starbucks Page if Starbucks has bid on the word "coffee".

3.3 Offsite Ad-Serving

In June 2012, FB-I began serving ads on third-party sites to Facebook users for the first time. These are the same ads the user would see on Facebook, and, as with all advertising on Facebook, no personal data of users is shared with the third-party site. No new ad-targeting criteria are used either. Only Marketplace ads and sponsored stories are displayed on third-party sites. Facebook ads and sponsored stories are shown through an i-frame on the third-party site. When a user logs into the third-party site with his or

her Facebook login, the iframe recognizes that that the user is logged into Facebook so personalized ads and sponsored stories can then delivered to the user, just as if the user were logged into facebook.com directly. The third-party site receives the same types of ad reporting that it would if its ads were served on Facebook. Facebook ads and sponsored stories on third-party sites function exactly as they do on Facebook. People can continue to report ads. They can also engage with these ads and sponsored stories just as they would on Facebook. In addition, FB-I has created content in its Help Center that is linked to directly from the ads so people can get more information about why they are seeing these ads.

FB-I describes this type of advertising its Data Use Policy:

> We may serve ads, including those with social context (or serve just social context), on other sites. These work just like the ads we serve on Facebook - the advertisers do not receive any of your information. Only people that could see the Facebook action (like on your timeline) would see it paired in this way.

3.4 Social Ads

As discussed above in section 2.4, the DPC recommended that the setting for users to exercise control over appearing in social ads be integrated into a user's privacy settings as opposed to being part of account settings. FB-I made that change, and now these settings can be found along with the other privacy settings.

3.5 Restrictions on Ad-Targeting Relating to "Sensitive Data"

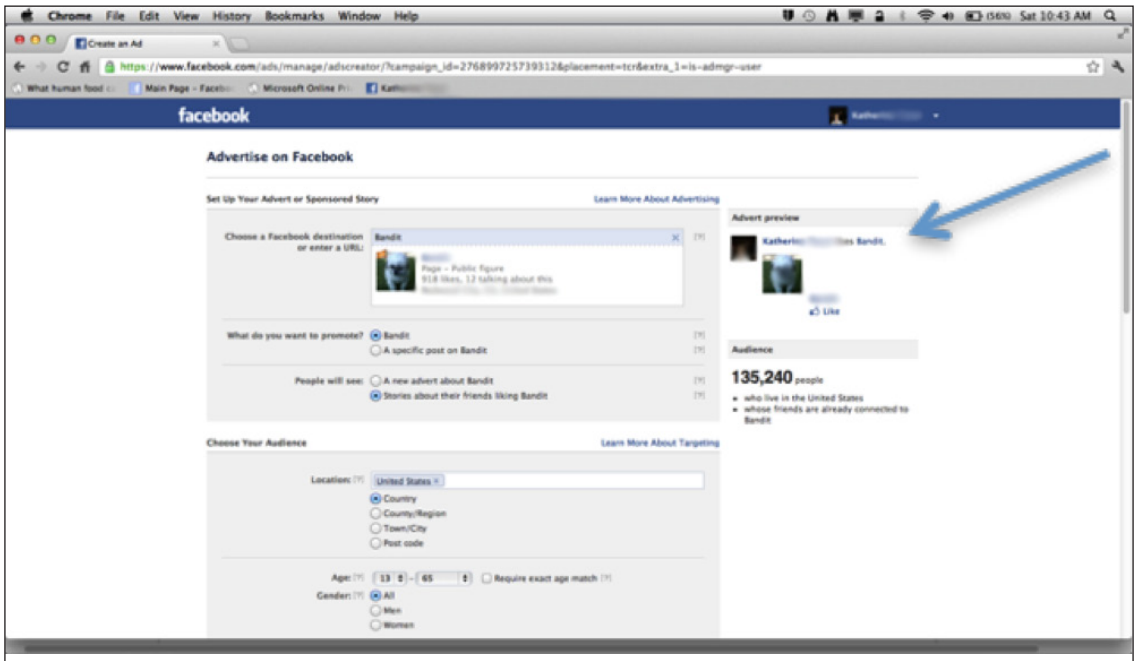
As the DPC noted in the Report on Audit, FB-I's Advertising Guidelines prohibit targeting based on a user's personal characteristics within sensitive categories. FB-I undertook to clarify its policy in this respect, which is to allow targeting on the basis of keywords entered by the advertiser but not allow targeting based upon the described categories of sensitive data. FB-I gives effect to this policy by not using any sensitive categories on the user's timeline as targeting criteria. For example, if a user fills in the "religious beliefs" field in his timeline, FB-I does not use that data for ad-targeting purposes.

3.6 Sponsored Stories

The DPC recommended that FB-I clarify further that a user's profile photo was public information, and therefore might be seen within a sponsored story. The revised Data Use Policy states: "Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public. Learn More." The "Learn More" link takes the user to the specific section entitled "Information that is always publically available," which includes:

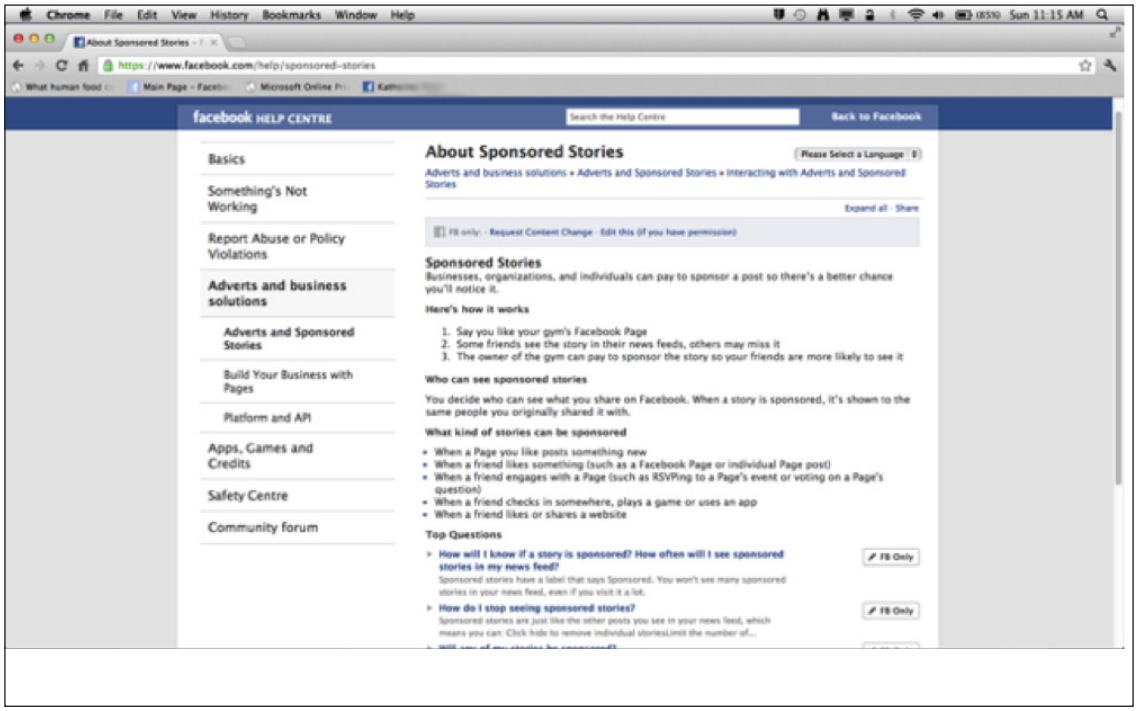
> **Profile Pictures and Cover Photos**
>
> These help your friends and family recognize you. If you are uncomfortable making any of these photos public, you can always delete it. Unless you delete them, when you add a new profile picture or cover photo, the previous photo will remain public in your profile picture or cover photo album.

Sponsored stories are simply posts that would appear in the News Feed anyway, but which advertisers can "sponsor" in order to increase the potential visibility of the story. For example, if a user "likes" The Irish Times Page, the user's friends could see a story of that "like" either organically, or as a sponsored story. In either case, the user's profile photo would be paired with the "like" action. See screenshot below:



There is also megaphone icon next to sponsored stories, which, when clicked, takes the user to a special page with easy-to-understand and comprehensive information about advertising on Facebook (see https://www.facebook.com/about/ads/. See screenshots below:

FB-I also added sponsored stories to the newsfeed and included a "sponsored" link directly in the story. The link takes the user to additional information about sponsored stories. See https://www.facebook.com/help/sponsored-stories. See screenshots below:



3.7 Ad targeting below 20 users

The DPC had some concern that Facebook advertising could be used as a means to target a specific individual through the very specific selection of user criteria. The DPC was satisfied, following the audit, that FB-I has put adequate safeguards in place to prevent this from occurring. Ads are only delivered based on targeted criteria when the audience reaches more than 20.

3.8 Information Available to Advertisers

A frequent question that arises in public comment is whether user information is made available to advertisers. FB-I clearly states that it does not share user information with advertisers without user permission. The DPC was satisfied that FB-I does not provide user data in breach of its Data Use Policy, but expressed a concern about the possibility of passive transmission of data such as an IP address when an advertiser has deployed a click tag (web beacon). In response to the DPC's concern, FB-I has increased transparency in its Data Use Policy, disclosing that:

> Most companies on the web use cookies (or other similar technological tools), including our advertising and Platform partners. For example, our Platform partners, advertisers or Page administrators may use cookies or similar technologies when you access their apps, ads, Pages or other content.

FB-I's Data Use Policy also lets users know how to exercise choice over the use of such cookies and other technologies:

> To learn more about how advertisers generally use cookies and the choices advertisers provide, visit the Network Advertising Initiative, the Digital Advertising Alliance, the Internet Advertising Bureau (US), or the Internet Advertising Bureau (EU).
>
> You can remove or block cookies or other similar technologies or block or remove other data stored on your computer or device (such as by using the various settings in your browser), but it may affect your ability to use Facebook or other websites and apps.

Furthermore, in June 2012, FB-I introduced a new "cookies statement" (see https://www.facebook.com/help/cookies), which is presented to users at the same time as the Data Use Policy and Statement of Rights and Responsibilities at registration, as well as provided through a link at the bottom of every page and at the right-hand side of the user's home page. The cookies statement details FB-I's use of cookies and other similar technologies, but also contains an FAQ about third parties' use of such technologies on FB-I and provides direct links to those third parties' sites, where users can exercise choice. See https://www.facebook.com/help/?faq=15996711079837 3#How-do-third-parties-use-cookies,-pixels,-and-other-similar-technologies-on-Facebook.

FB-I permits advertisers to use tags. Click tags send information to the advertiser when the user clicks on the ad and contain a random id for the user (not their Facebook user id). View tags send information to the advertiser when a user views the ad. Both of these tags permit the placement of cookies on a user's browser.

In addition to Facebook's Advertising Guidelines, which prohibit the use of user data derived from ads served on Facebook for any purpose other than for anonymous measurement, since January 2011, FB-I has implemented a new policy that requires tracking technology providers that place tags in Facebook-served ads to be approved by FB-I. This is an industry-leading practice as most publishers do not impose these restrictions on third-party ad servers. To be approved, tracking technology providers are requested to sign and comply with an advertising data protection agreement. Under this agreement, they may only drop one cookie. That cookie may only be used only to track the clicks and the impressions. It may not collect any other information, such as personal information about the user or targeting criteria. It also explicitly prohibits tracking technology providers from creating users' profiles or from using any data obtain through Facebook to re-target users with ads outside of Facebook.

FB-I also has automated monitoring practices in place to check that ad creatives do not contain unauthorized tags and that platform developers are using approved ad networks.. The team is typically able to identify if the tag comes from an approved vendor or not.

As mentioned above, in June 2012, FB-I introduced its cookies statement, which offers users the ability to exercise increased choice over whether third parties can place cookies on their browsers. FB-I has made the process very easy for users by providing a list of the most-used ads technology companies with a link that goes directly to the opt-out section of the third party's website.

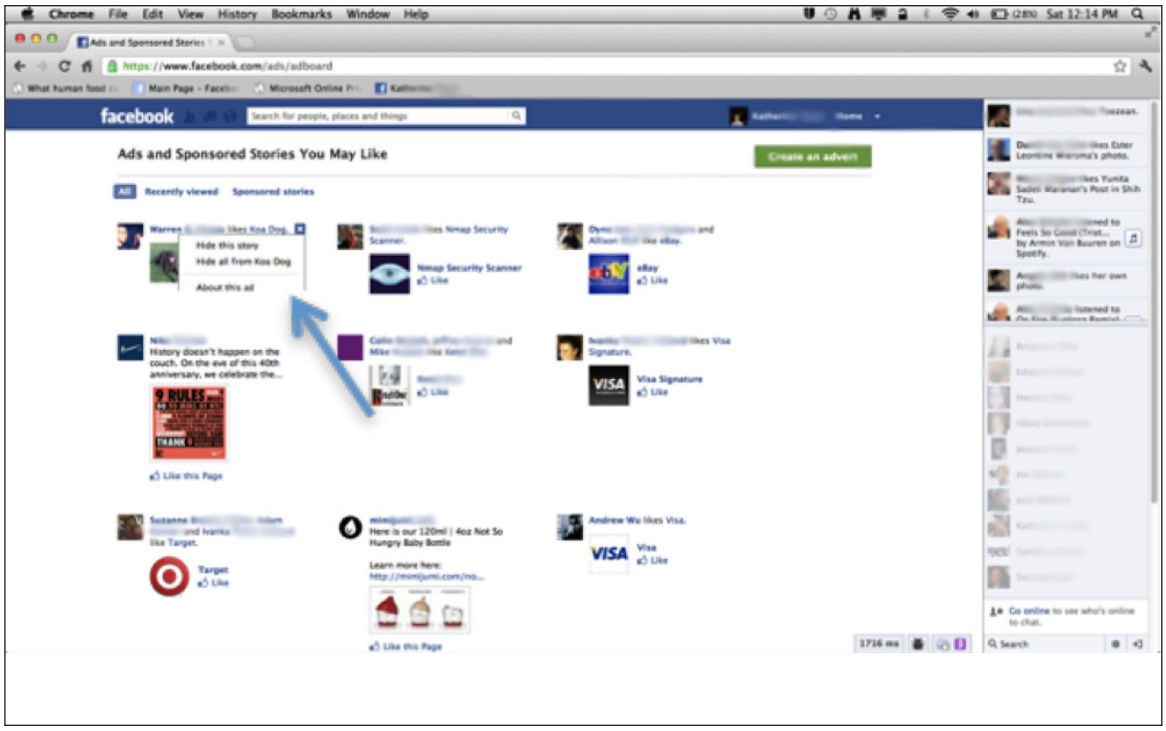
3.9 Retention of Ad-Click Information

The DPC recommended that FB-I have a retention policy for ad-click data. FB-I has implemented a policy whereby user-identifiable ad-click information that is needed for legal or regulatory reasons for periods longer than two years will be copied out of the main storage database and be saved only for such purposes. Such data will not be accessible to or usable by any employees except for those who need to access it for the purposes it is maintained. FB-I is anonymising all ad-click data in the main storage database after a two-year period. FB-I states that the two-year period is necessary: 1) to honour user requests (for example, when a user indicates that he or she does not want to see a particular ad, or an ad from a particular advertiser), 2) to resolve disputes with advertisers, and 3) to improve the overall quality and relevance of ads shown to its users.

3.10 User Influence Over Ads Displayed

FB-I offers users the ability to influence the ads they see. This feature has been available by clicking the "x" that appears next to FB-I advertising and enables the user to prevent that ad from reappearing, or to block all advertisements from the responsible company. The DPC indicated that this feature did not appear to be well known to users and recommended that FB-I educate users better. In response to this recommendation, FB-I added a section on influencing the ads one sees to its About Advertising page, which is accessible by clicking on the megaphone icon in an ad. See screenshot below:

The link "adverts you see on Facebook" takes the user to a page that shows the user many of the recent ads the user has been shown and gives the user the ability, in one place, to influence whether the ad or the ad type is shown again. See screenshot below:



FB-I also has extensive information about how advertising works and how to influence the ads that are displayed in a link on the Data Use Policy. See https://www.facebook.com/help/?page=226611954016283.

FB-I endeavors to show users the most relevant and interesting ads possible. It does so by using a range of user data – primarily the user's stated likes and interests. However, when FB-I's ad-targeting fails to display an ad that appeals to a user, FB-I gives the user the ability to provide feedback, and, in doing so, to influence the ads that are displayed in the future.

Chapter 4 – Access Requests

The right for an individual to access personal data held by a data controller established in the EU is a basic right enshrined in the Data Protection Acts and the EU Data Protection Directive. The right of access grants a means for an individual to establish (subject to limited restrictions) within 40 days what data is held about them and to seek correction or deletion where this may be necessary.

In the Report of Audit, the DPC expressed that "… the key requirement in response to an access request is to ensure that a user has access to their personal data. Therefore, either the data must be available on the requester's profile page, their activity log, which is a feature of the new user Timeline, or via the download tool. From a transparency perspective, it is desirable that most, and ideally all, of a user's data should be available without having to make a formal request. FB-I therefore will be implementing a number of enhancements to the activity log to provide users with access to and control over information about them."

As FB-I noted in its response in the Report of Audit, "[t]he complex issues around subject access requests are particularly challenging for FB-I. Our wide user base means that we could, theoretically, be subject to hundreds of millions of such requests. In addition, our platform is distributed and decentralised in nature, with no one single "file" containing the totality of each user's personal data."

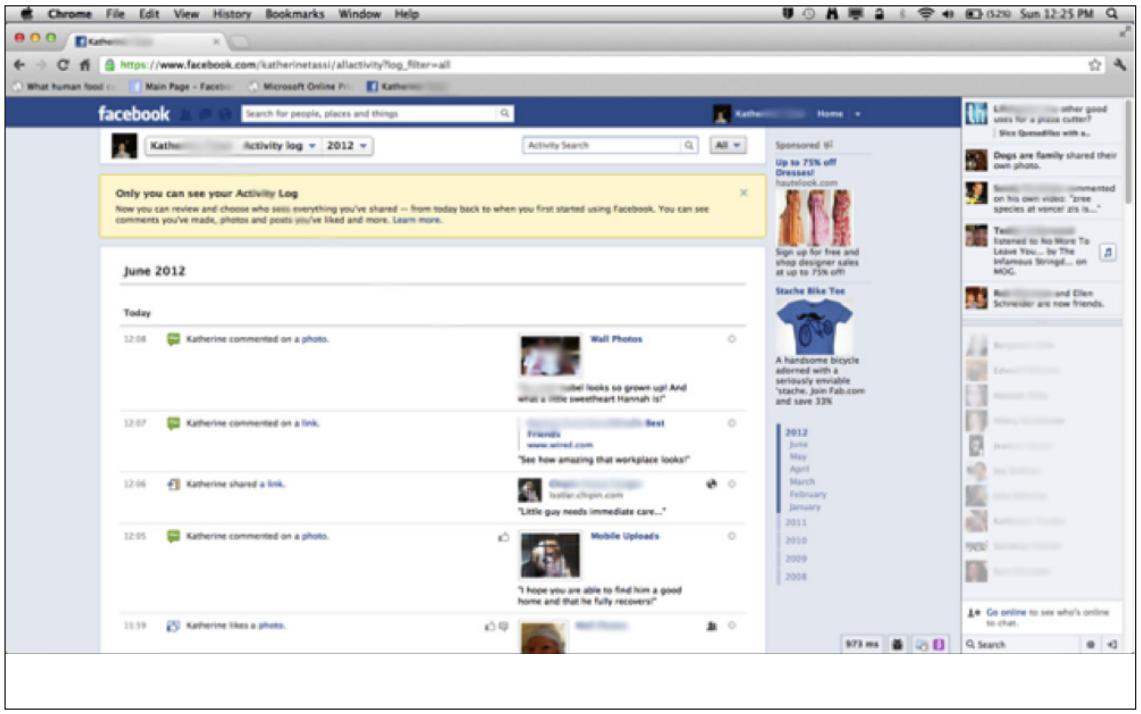
During the course of the audit, FB-I has been continually revising and refining its subject access request process to make it easier to use. We have created a new, dedicated page where any user or non-user can make a subject access request.

FB-I has approached its responsibility to ensure full access to data for all its users very seriously and has worked diligently at building a self-service tool to supplement the existing mechanisms available to users to access their data. FB-I's commitment to transparency, access, and control can be seen by its extraordinary efforts to make users' personal data easily available to users rather than requiring users to correspond with FB-I to make a request and wait up to 40 days for a response. FB-I decided that where it was possible to surface user data directly in users' accounts via the timeline or Activity Log, it would do so and thereby give users control over indivdually deleting the data in most cases.

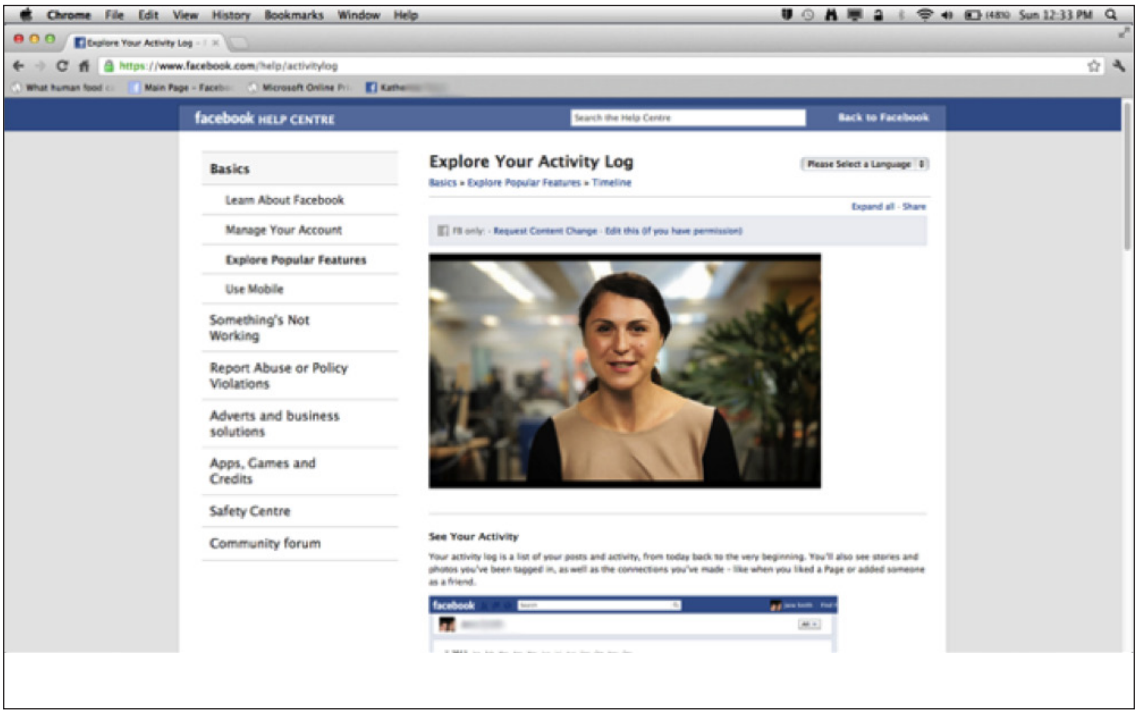
Section 4 of the Data Protection Acts

4.1 User Activity Log

Facebook's Activity Log provides unprecedented, industry-leading transparency into the historical actions taken by the user on the site. The Activity Log can be seen only by the user, and from the log itself, users can control the visibility of each action – whether it is visible on the user's timeline or not – and can delete almost every item on a per-item basis. Categories of action can be isolated so that a user can search only his or her comments on others' posts for example. See screenshot below:



The "learn more" link takes the user to extensive help center information on Activity Log. See https://www.facebook.com/help/activitylog. See screenshot below:



4.2 Expanded Archive

For a large amount of data that is perhaps of somewhat less interest to users on a regular basis, FB-I engineered a second download tool, called "expanded archive", from which users can access largely historical data. The previously existing download tool still provides users with a vast amount of data,

some of which is supplied in other places as well. FB-I spent the six months between the publication of the Report of Audit and July 2012 examining every piece of user personal data it holds and figuring out how to make it available to users. The project entailed enormous engineering efforts and resulted in an unprecedented amount of data being easily available to users. FB-I is not aware of any other web service that provides individuals access to their data as comprehensively and easily as it does.

4.3 Data Available

The DPC in the Report of Audit made reference to the complaint of the organization "Europe v. Facebook" regarding 19 supposed categories of data that FB-I did not make available to users. FB-I and the DPC examined each of these supposed categories of data throughout the audit process. The following is a list of the categories and the outcome (many categories of data are available in multiple places):

- Content posted on other's pages: *available in Activity Log*
- Videos posted: *Available in Activity Log and on timeline*
- Use of 'like' button: *Available in timeline and in Activity Log*
- Browser type: *Available in Expanded Archive*
- Interaction with advertisements: *in Expanded Archive*
- Conversion tracking: *as interpreted, such data is kept in aggregate form only*
- Indicates a friendship: *unclear as to what this means*
- Pictures where tag removed: *in Activity Log*
- Tracking information on use of other websites: *Facebook does not track users on other websites; insofar as FB-I receives data via social plugins, such data is anonymized within 90 days; during the 90-day period, it is inaccessible for per-user extraction of data.*
- Searches made: *will be added to Activity Log or Expanded Archive*
- Settings: *existing setting in user's account; Facebook does not store historical settings*
- Click flows: *unclear what this means, but insofar as it means ad clicks, unavailable due to inaccessibility of storage location for per user extractions*
- Use of 'friend finder': *in Expanded Archive*
- Outcomes from matching, face recognition and ad-targeting processing: *underlying algorithm calls for intellectual property/trade secret information; facial composite is in Activity Log*
- Use of pictures by face recognition tool: *facial composite is in Activity Log*
- Data gathered from another's 'synchronisation': *as far as understood, this is other users' data stored in other users' accounts*
- Relationship with other users: *in Expanded Archive and on timeline*
- Reaction of other users to content posted: *comments on user's posts in Activity Log*
- 'Invitations' sent and received: *in Activity Log, in user's account*

In total, the personal data available to users is described, along with where it can be found, in the following chart, which is available to users at https://www.facebook.com/help/?page=116481065103985. The Help Center also contains FAQs providing information about downloading and accessing one's personal data on Facebook.

This is the data users can find, a short explanation of what it is and where they can find it (downloaded info, expanded archive or activity log). FB-I stores different types of data for different time periods, so FB-I may not have all of a user's data since he or she joined Facebook. FB-I also does not surface in the downloaded data certain data, like passwords, for security reasons or transitory scores that help with troubleshooting, assessing site integrity, risk, or violations of our Terms.

What info is available?	**What is it?**	**Where can I find it?**
About Me	Information you added to the About section of your timeline like relationships, work, education, where you live and more. It includes any updates or changes you made in the past and what's currently in the About section of your timeline.	Activity Log
Account Status History	The dates when your account was reactivated, deactivated, disabled or deleted.	Expanded Archive
Active Sessions	Contains all stored active sessions, including date, time, device, IP address, machine cookie, and browser information.	Expanded Archive
Ad Clicks	Dates and times and title of ads clicked.	Expanded Archive
Address	Your current address or any past addresses you had on your account.	Expanded Archive
Ad Topics	List of topics that you may be targeted against based on your stated likes, interests, and other data you put in your timeline.	Expanded Archive
Alternate Name	Any alternate names you have on your account (ex: a maiden name or a nickname).	Expanded Archive
Apps	All of the apps you subscribe to.	Expanded Archive
Birthday Visibility	How your birthday appears on your timeline.	Expanded Archive
Chat	A history of the conversations you've had on Facebook Chat.	Downloaded Info
Check-ins	All of the places you've checked into.	Downloaded Info
City and Hometown	The current city where you indicate you live and the hometown you indicate in your timeline.	Activity Log
Connections	The people who have liked your Page or Place, RSVPed to your event, installed your app or checked in to your advertised place within 24 hours of viewing or clicking on an ad or Sponsored Story.	Timeline and Expanded Archive
Credit Cards	If you make purchases on Facebook (e.g., in apps) and have given Facebook your credit card number.	Activity Log
Currency	Your preferred currency on Facebook. If you use Facebook Payments, this will be used to display prices and charge your credit cards.	In your account when you log in
Current City	The city you added to the About section of your timeline.	Expanded Archive
Date of Birth	The date you added to Birthday in the About section of your timeline.	Downloaded Info
Deleted Friends	The people you've unfriended.	Downloaded Info
Education	Any information you added to Education in the About section of your timeline.	Expanded Archive

What info is available?	What is it?	Where can I find it?
Emails	Email addresses added to your account (even those you may have removed).	Downloaded Info
Events	Events you've joined or been invited to.	Expanded Archive
Family	Friends you've indicated are family members.	Activity Log
Favorite Quotes	Information you've added to the Favorite Quotes section of the About section of your timeline.	Expanded Archive
Friend Requests	Pending sent and received friend requests.	Downloaded Info
Friends	A list of your friends.	Expanded Archive
Gender	The gender you added to the About section of your timeline.	Downloaded Info
Groups	A list of groups you belong to on Facebook.	Downloaded Info
Hidden from News Feed	Any friends, apps or pages you've hidden from your News Feed.	Downloaded Info
Hometown	The place you added to hometown in the About section of your timeline (profile).	Expanded Archive
IP Addresses	A list of addresses where you've logged into your Facebook account (won't include all IP addresses as they are deleted according to a retention schedule).	Downloaded Info
Last Location	The last location associated with an update.	Expanded Archive
Likes on Other's Posts	Posts, photos or other content you've liked.	Activity Log
Likes on Your Posts from others	Likes on your own posts, photos or other content.	Activity Log
Likes on Other Sites	Likes you've made on other sites off of Facebook.	Activity Log
Linked Accounts	IM names, etc., if you have linked them to your Facebook account	Activity Log
Locale	The language you see on Facebook is based on where you're located.	In your account when you log in
Logins	IP address, date and time associated with logins to your Facebook account.	Expanded Archive
Logouts	IP address, date and time associated with logouts from your Facebook account.	Expanded Archive
Messages	Archive of messages you've sent and received on Facebook and that you have not deleted. Note, if you have deleted the message and the recipient or sender has not, the message will not be included in your download.	Expanded Archive
Name	The name on your Facebook account.	Downloaded Info
Name Changes	Any changes you've made to the original name you used when you signed up for Facebook.	Downloaded Info
Networks	Networks (affiliations with schools or workplaces) that you belong to on Facebook.	Expanded Archive

What info is available?	What is it?	Where can I find it?
Notes	Any notes you've written and published to your account.	Expanded Archive
Notification Settings	A list of all your notifications and whether you have email and text enabled or disabled for each.	Activity Log
Pages You Admin	A list of pages you admin.	Expanded Archive
Pending Friend Requests	Pending sent and received friend requests.	Expanded Archive
Phone Numbers	Mobile phone numbers you've added to your account, included verified mobile numbers you have added for security purposes	Expanded Archive
Photos	Any photos you've uploaded to your account.	Expanded Archive
Photos Metadata	Any metadata that is transmitted with your uploaded photos	Downloaded Info
Physical Tokens	Badges you've added to your account.	Pending, will be added to Expanded Archive
Pokes	A list of who's poked you and who you've poked.	Expanded Archive
Political Views	Any information you added to Political Views in the About section of timeline.	Expanded Archive
Your Posts	Anything you posted to your own timeline, like photos, videos and status updates.	Downloaded Info
Posts by Others	Anything you posted to someone else's timeline (profile), like photos, videos and status updates.	Activity Log
Privacy Settings	Only current settings are stored.	Activity Log
Recent Activities	Actions you've taken and interactions you've recently had.	In account when you log in.
Registration Date	The date you joined Facebook.	Activity Log
Religious Views	The information you added to Religious Views in the About section of your timeline.	Activity Log
Removed Friends	People you've removed as friends.	Downloaded Info
Screen Names	The screen names you've added to your account, and the service they're associated with. You can also see if they're hidden or visible on your account.	Activity Log
Searches	Searches you've made on Facebook.	Expanded Archive
Shares	Content, such as a news article, you have shared with others on Facebook using the "share" button or link.	Coming soon in Activity Log
Spoken Languages	The languages you added to Spoken Languages in the About section of your timeline.	Activity Log
Status Updates	Any status updates you've posted.	Expanded Archive
Subscribers	A list of people who are subscribed to you.	Activity Log
Subscriptions	A list of people you subscribe to.	Expanded Archive

What info is available?	What is it?	Where can I find it?
Tag Suggestions Template	A unique number based on a comparison of the photos you're tagged in. We use this template to help your friends tag you in the photos they upload.	Activity Log
Work	Any information you've added to Work in the About section of your timeline.	Expanded Archive
Vanity URL	Vanity name for your account.	Downloaded Info
Videos	Videos you've posted.	Visible in URL on your timeline homepage

4.4 Responses to Existing Access Requests

As the DPC noted in the Report of Audit, FB-I received over 40,000 access requests during a very short period of time prior to the audit. FB-I worked hard to notify all of those individuals who had made access requests of: 1) the agreement FB-I reached with the DPC regarding access requests as a result of the audit, and 2) when FB-I added further categories of data to the download tool.

Chapter 5 – Data Retention

The Report of Audit stated: "Data retention is a standard issue considered during the course of all audits conducted by this Office. Section 2(1)(c) of the Data Protection Acts 1988 & 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. In determining appropriate retention periods for personal information, data controllers can have due regard to any statutory obligations to retain data. However, if the purpose for which the information was obtained has ceased and the personal information is no longer required for that purpose, the data must be deleted or disposed of in a secure manner. Full and irrevocable anonymisation would achieve the same objective. Given the nature of the retention obligation which can be subjective in many respects, the identification of acceptable retention periods is one of the more discussed and debated issues in the conduct of audits and investigations by this Office."

The DPC further noted, "The complexity of an information society service such as FB-I makes it a continuing challenge for it to define and identify data which can be considered to be personal data and apply appropriate retention periods to each category of such data. FB-I has committed to do so on an ongoing basis.

"FB-I has noted that its success depends upon constantly innovating and constantly providing better and better experiences for users. At its most basic formulation, this includes showing users the information that they most are interested in, whether it be content from their friends or others or music or news shared by others or advertisements that are most relevant to them. It also includes shielding users from negative experiences like multiple unwanted friend requests, or harassment or bullying of any kind.

FB-I has highly complex systems to provide such positive experiences and block negative ones. Most of these systems require that FB-I retain user data. Such data is used for the purpose of providing the service users expect when they come to Facebook. FB-I expresses this explicitly in its Data Use Policy:

> We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, we may use the information we receive about you:
>
> - *as part of our efforts to keep Facebook safe and secure;*
> - *to provide you with location features and services, like telling you and your friends when something is going on nearby;*
> - *to measure or understand the effectiveness of ads you and others see;*
> - *to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it.*
>
> *Granting us this permission not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.*

FB-I's policy is to make data retention decisions in conformity with Irish law based on its understanding of the expectations of the people who use Facebook as well as the length of the time that it needs the data to provide a quality experience on Facebook and to understand and improve the service it offers.

FB-I noted that its retention policies in any of these contexts may be over-ridden by a legal requirement, a regulatory obligation, or an ongoing investigation into abuse, but only for as long as that reason lasts."

Indeed, FB-I has spent the past six months evaluating all of the personal data of users that it receives precisely to determine whether a set retention period is appropriate or whether retention should be approached more flexibly – something to be evaluated on a regualar basis to ensure that the purposes for which FB-I has the consent of users to use the data still exist.

5.1 Retention of Log of "Removed" Data

In the Report of Audit, the DPC noted the specific complaints by the "Europe v. Facebook" group to the retention of data that appeared to the group to have no purpose after a user "removed" the data from his or her profile. Such data included: removed tags, removed friends, former groups, and deleted posts. FB-I's response noted that it saved removed pokes, tags, groups and friends for user experience reasons, but agreed that it could provide greater transparency to users and greater control where possible over the deletion of data.

FB-I still regards it as a necessity to retain data related to actions users take, like removing tags and removing friends – this enables FB-I to prevent re-tagging after a user has expressed a desire not to be tagged and prevent the suggestion to a user to friend someone he or she has removed as a friend. However, FB-I now provides users with access to this stored data, as well as other actions, such as "unliking" a page the user previously liked. From the Activity Log, where this data is displayed, users can also delete the data if they so wish albeit in doing so they may be re-tagged in the content.

5.2 Deletion of Messages

FB-I enables messages to be sent directly from one user to one or more other specified users. In these instances, the sender and each recipient can access a copy of the message in his or her account, and FB-I retains a copy of that message in order to permit this access. In the Report of Audit, the DPC expressed that FB-I's policy and practice to delete a message entirely after all parties to the communication have deleted their copies of the message was an acceptable approach. The DPC indicated that this approach would be confirmed during the July review.

"The approach of this Office in relation to retention is that all periods chosen for the retention of personal data must be fully evidence based and the period chosen cannot seek to cover all possible eventualities where personal data may be useful to the company. We have applied the same approach to FB-I which has sought in response to identify retention periods which meet this objective."

5.3 Social Plugin Impression Log Data and Cookies

FB-I's new retention policy with respect to impression log data and cookies is as follows:

- For people who are not Facebook users or who are Facebook users in a logged-out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits facebook.com.
- For all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin.

This approach allows FB-I to retain information about social plugins from logged-in users to improve the social plugin experience, briefly use it in the aggregate to make Page recommendations, and to identify and resolve any technical issues in the operation of the service, and then eliminate it once FB-I does not need it for those purposes.

Social plugin impression data was the subject of a legal hold on the part of Facebook, Inc. in December 2011 and July 2012 due to class action litigation against Facebook, Inc. The litigation potentially implicated all users worldwide as class members. In an abundance of caution, Facebook, Inc., had accordingly retained logs that it would otherwise have deleted, in the event that material became relevant to the litigation. Facebook, Inc., has since learned that it does not need to retain such data for European users and is in the process of determining a timeframe within which it can delete the stored data, which involves first isolating the logs with IP addresses from European countries.

5.4 Search Data

During the audit in December 2011, FB-I proposed a retention policy of six months for user-identifiable search logs. FB-I has begun anonymizing historical search logs. Since that time, FB-I has determined that historical user-identifiable search queries, as opposed to logs, are necessary to improve and deliver to users the ability to search effectively on Facebook. Historical user-specific search queries are vital to the development and delivery of our search product, as well as being critical to maintaining and improving the Facebook experience. In the alternative to a set retention period for such queries, Facebook will give users control over the retention of their search queries.

This is in keeping with FB-I's model of data transparency, accessibility, and control for users. FB-I believes that giving users control over the retention period of data strikes a fair balance between permitting FB-I to use the data for its legitimate business purposes of product improvement and delivery and offering users who object to further processing of the data the opportunity to delete it.

5.5 Ad-Click Data

As discussed in section 3.10 above, FB-I has developed a policy that it will anonymise ad-click data after 2 years. Ad-click data that it must retain for regulatory or legal reasons in a user-identifiable form will be copied into a separate database and used only for the regulatory or legal reasons it is needed. Furthermore, readily available ad-click data will be provided to users in their expanded archive download.

5.6 Login Information

FB-I retains information in relation to the login activity of users. FB-I does so primarily for security purposes. This includes the date, time, IP address used, browser, operating system information and security cookie information from every such login by a user. In response to the DPC's recommentation to enhance the information available in this regard, FB-I added to the section "Other information we receive about you" in its Data Use Policy the following:

> We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby.

During the audit in December 2011, FB-I provided the DPC with an appropriate evidence base to justify the retention period, although the precise details were not published so as not to undermine security. FB-I has implemented the agreed-upon retention period.

5.7 Deactivated and Inactive Accounts

During the audit and throughout the past six months, FB-I has considered carefully the consequences of having a set retention period for accounts users choose to deactivate temporarily or accounts users are not actively using. Indeed, FB-I has been in a number of conversations with the DPC to explain its conclusion that such accounts should not be subject to a set retention period because users themselves have complete control over the retention or deletion of their accounts. In the Report of Audit, the DPC

stated, “Now that FB-I has matured to an established company there remains an issue to be addressed in relation to how long FB-I should continue to hold user accounts where no activity has taken place or where the user deactivated his or her account. An appropriate solution must be found so as to ensure that FB-I does not continue to hold such personal data after the purpose for which the data was collected has expired. One approach would be to adopt a hard policy of say one year after the last activity or where a deactivation request was made and delete all such accounts. This could be highlighted in the Data Use Policy and appropriate email reminders could be sent to a user prior to formal deletion. One obvious flaw in this approach is that certain members of society, e.g. prisoners may be precluded from accessing FB-I and indeed email during their stay in prison and it would appear disproportionate to delete their information when they would not be in a position to offer a view. As well, users could be travelling or engaged in some other activity during which time they have chosen not to be active on FB-I. This therefore is a complex issue and one on which this Office intends to have further discussions with FB-I.”

In reaching its conclusion that a retention period for deactivated and inactive accounts would be contrary to the expectations of users, FB-I carefully examined the available data on user re-activations, reasons given for deactivating accounts, and account inactivity periods. The Facebook service is still comparatively young – it is less than six years old as a worldwide service (Facebook opened the service up to everyone 13 and over with an email address on September 26, 2006.) Nevertheless, the data shows that 1) the majority of users who deactivate expressly indicate that they are doing so temporarily; 2) the majority of users who deactivate reactivate their accounts, with the longest periods of deactivation being over two years; and 3) a substantial number of accounts that appear inactive for over two years become active again. Given that users store some of their most treasured and personal information on Facebook – vast numbers of photos, communications with friends and families – FB-I cannot justify unilaterally deleting either deactivated or inactive accounts.

Facebook offers users a clear choice between deleting and deactivating their accounts. The difference between the two options is described in the Data Use Policy. The policy also makes an express promise that the deactivated account will remain stored with Facebook until a user returns: “Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future.”

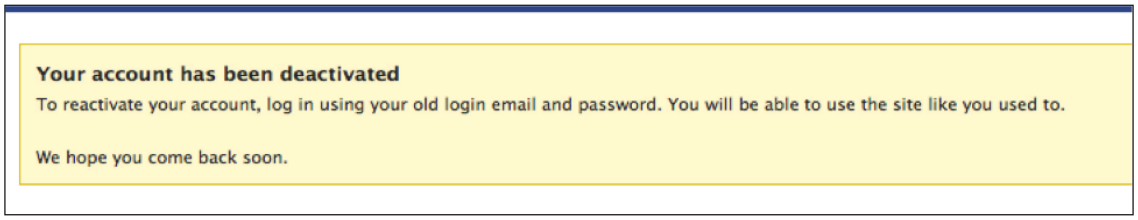
There can be no confusion whatsoever on the user’s part that deactivating one’s account will keep the account in storage for the user. Deactivation is a user-friendly option; FB-I makes it easy for users to be active on Facebook, and then, when they want to stop using their accounts, but don’t want to delete them forever, FB-I makes it easy for users to put their accounts on hold. Facebook stores the account but it is no longer visible on Facebook. As soon as the user logs back in to Facebook, their account is restored and visible again.

When a user chooses to deactivate his account, Facebook asks the user to select from the following reasons:

- I have a privacy concern.
- This is temporary. I'll be back.
- My account was hacked.
- I have another Facebook account.
- I spend too much time using Facebook.
- I don't feel safe on Facebook.
- I don't understand how to use Facebook.
- I don't find Facebook useful.
- I receive too many emails, invitations and requests from Facebook.

On a daily basis, hundreds of thousands of users reactivate their accounts.

When a user deactivates, the user is reminded that deactivation is putting the account on hold:



Users deactivate their accounts because they do not want these accounts to be deleted. When a user chooses to use the deactivate function, they do so in reliance on Facebook's representations that it will store the relevant information safely until the user decides to reactivate, or delete, their account.

Furthermore, FB-I makes no representations or disclosures to users that their accounts might be deleted if they are not actively using them. People with a Facebook account can be "passive" users since they receive notifications of activity on their accounts all the time (unless they have turned off all notifications). This means that Facebook users can be engaged with the activity in their accounts without ever visiting the site. They can view posts, photos, receive invitations, etc., from all of their friends for years, and yet they would appear "inactive" from the standpoint of logging in to the site. Indeed, they can communicate directly with their friends on Facebook through the notifications by choosing to respond via private email. Under its current terms, Facebook cannot unilaterally begin deleting "inactive" accounts.

As an alternative to deleting deactivated and inactive accounts after a period of time, FB-I has proposed: 1) to ensure that users who are inactive on Facebook continue to receive notifications at least annually reminding them of their accounts, and 2) after one year of not logging into Facebook, FB-I will notify the user that his or her account will be put into a state of deactivation. In this way, the account will not be visible on Facebook. Furthermore, FB-I will not process deactivated account data for any other purpose than storage and sending notifications to the account email. As well, FB-I will provide a means for individuals to check whether they have an old account on Facebook and recover it, if so, in order to continue using it, delete it, or deactivate it. Finally, FB-I will re-evaluate its policy regularly, especially as the service gets older and it is able to analyze patterns around deactivation and inactivity.

5.8 Deletion of Data from Incomplete Registration

One subject covered in the Report of Audit was establishing a retention period for data collected on the first screen of the registration process prior to the individual accepting FB-I's terms of service when the individual did not follow through and accept the terms ("abandoned registrations"). FB-I agreed to delete such data within 30 days if the individual did not come back to complete registration. Because FB-I changed its registration process so that individuals accept the terms of service before submitting any data, there are no longer any "abandoned registrations." All data collected is pursuant to FB-I's terms of service.

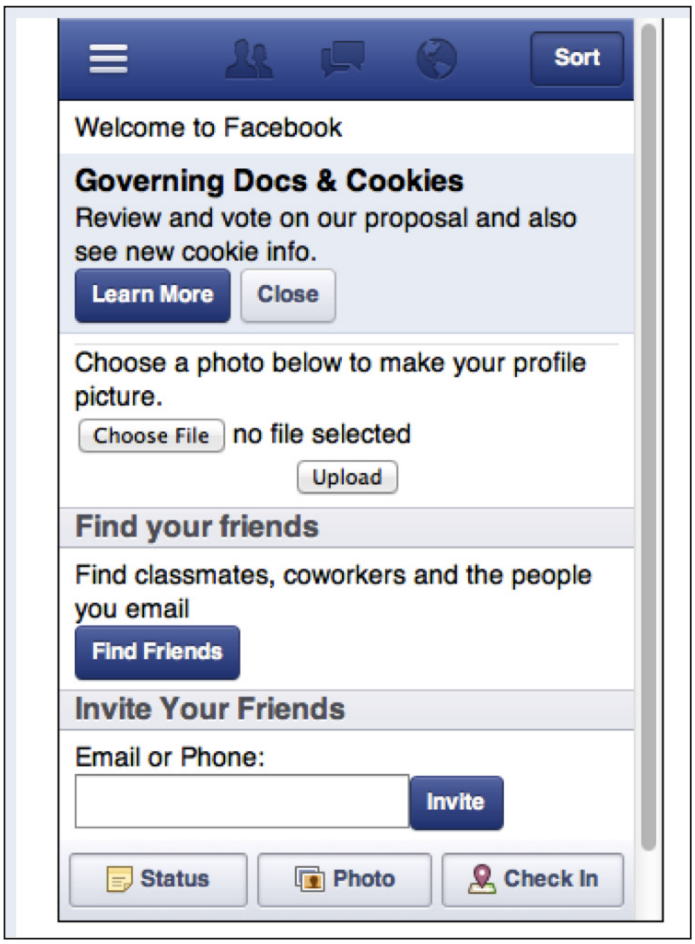
Chapter 6 – Cookies and Other Similar Technologies

In the Report of Audit and its Appendices, FB-I's use of cookies was described in great detail. Since the Report's publication, several developments have occurred.

6.1 Cookies Statement

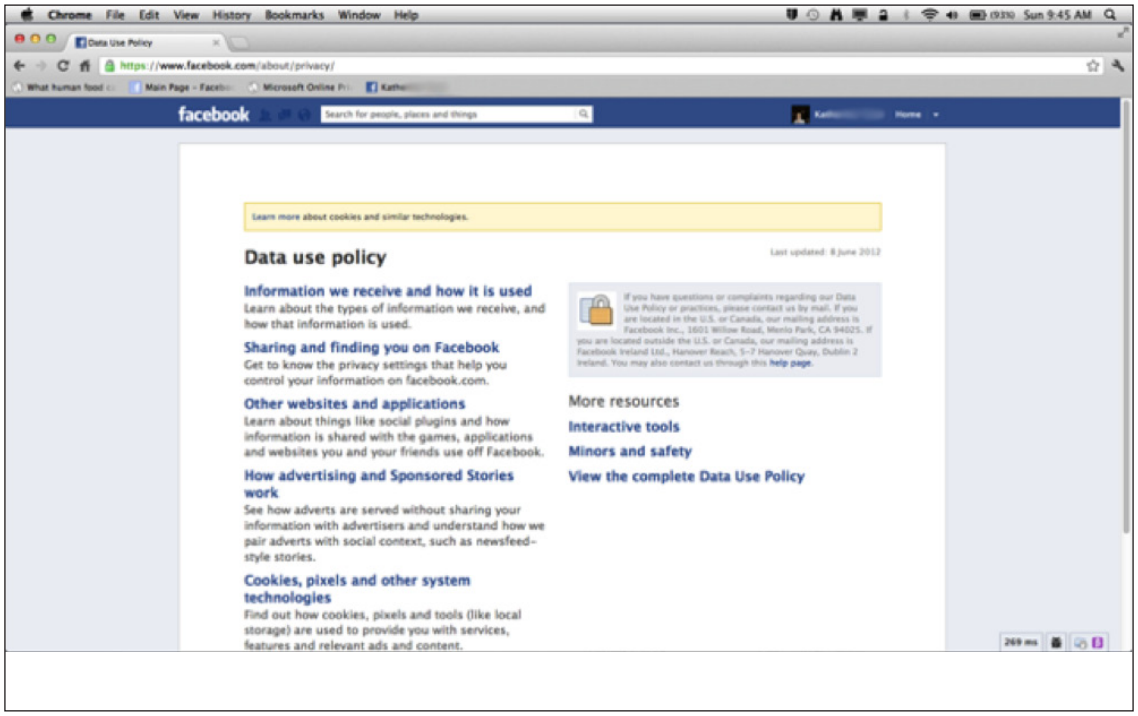
In June 2012, FB-I, cognizant of the requirements of the ePrivacy Directive, posted its cookies statement. The statement was added to the registration page, so individuals may read and agree to the use of cookies prior to registering for an account. A link to the cookies statement was placed in the revised Data Use Policy, at the bottom of the logged-out homepage, at the bottom of most pages on the site, and at the right-hand side of the homepage. Furthermore, FB-I provided all users, both on the web and on mobilewith notice of the cookies statement when it gave notice of the proposed revisions to the Data Use Policy. See screenshots below.

(on website)



(on mobile)

FB-I has also placed a banner across the top of the landing page for the Data Use Policy highlighting the cookies statement. See screenshot below:



FB-I also Expanded the information about cookies and other similar technologies in its Data Use Policy, giving that section a prominent heading on the landing page. See screenshot above.

FB-I's cookies statement describes the technologies used on the website, the types of cookies used, and the purposes. The statement provides even further information in a series of FAQs, including information about third parties' use of such technologies and direct links to the web pages where users can exercise choice over the cookies and other technologies FB-I and third parties use. See https://www.facebook.com/help/cookies and https://www.facebook.com/help/?faq=159967110798373#How-do-third-parties-use-cookies,-pixels,-and-other-similar-technologies-on-Facebook.

FB-I's cookies statement also provides a link to the Report of Audit, where users can read about the DPC's analysis of cookies on the Facebook site.

6.2 Social Plugin Data

As described in detail in the Report of Audit, Facebook uses cookies to enable Facebook users to have a social experience on third-party sites. No cookies are placed by social plugins, but rather, Facebook reads an existing cookie (placed when someone visits a Facebook webpage) when an individual visits a site with a social plugin. The information Facebook receives from this cookie (described in the Data Use Policy) is used to analyze the performance of social plugins and fix bugs. No data regarding a user's offsite browsing is stored in the user's profile, and such data is anonymized and deleted within 90 days.

Chapter 7 – Third-Party Apps

FB-I works to strike the right balance in terms of what protections and tools it should and can offer to users engaging with Platform applications and what obligations more appropriately rest with developers and users themselves. With hundreds of thousands of applications built on the Facebook Platform, FB-I must prioritize its efforts in ensuring an overall positive user experience when engaging with applications.

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 re-evaluating and improving its already impressive safety and security efforts.

Another important consideration is the user experience: providing easy and understandable access to applications on Platform. In its Report of Audit, the DPC expressed its opinion "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." As described below, FB-I has made significant efforts to do so.

Another consideration is ensuring developer compliance with FB-I's policies.

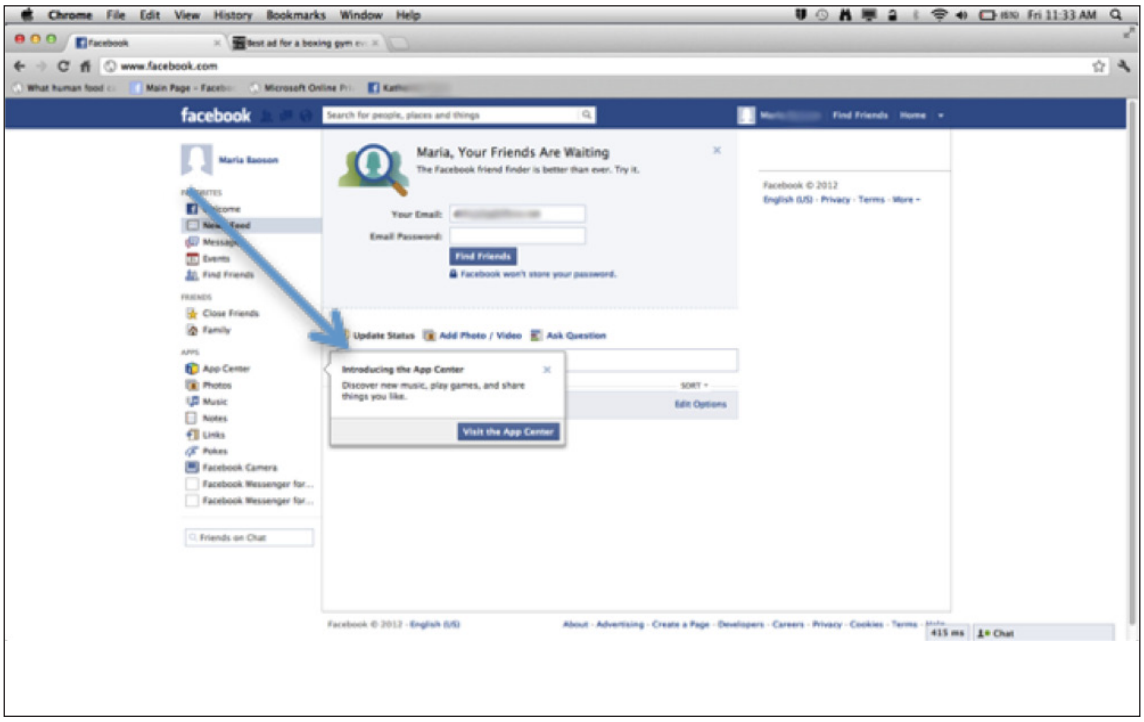
7.1 Safety and Security on Platform

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 tothis, 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.

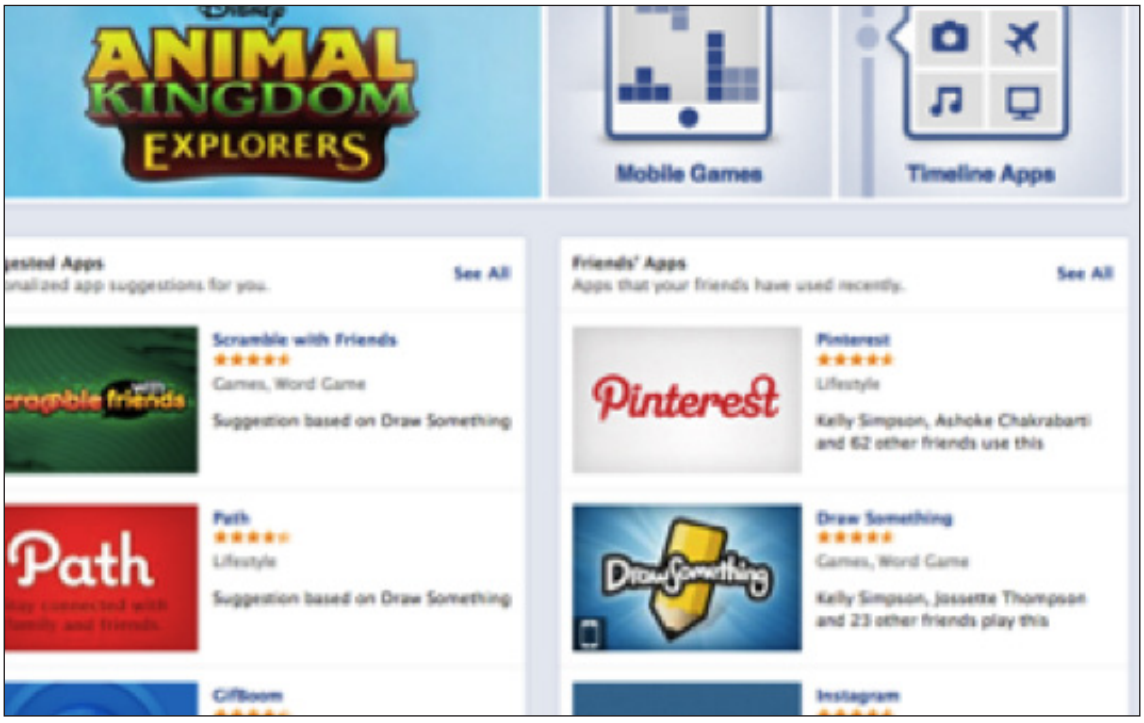
7.2 User Experience

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:



(part of the new user experience)



(landing page for app center)

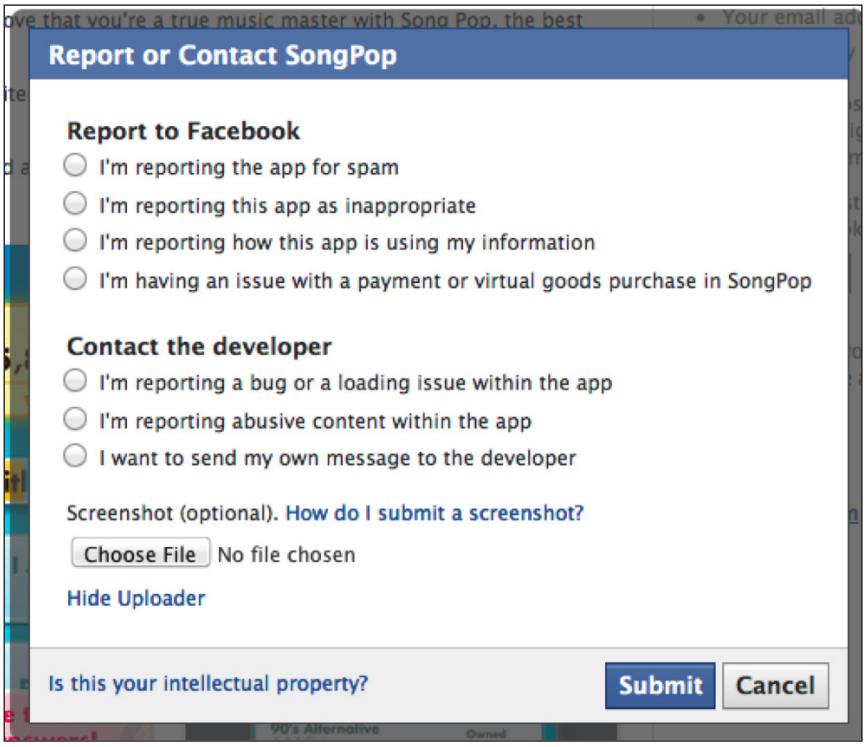
From the app's landing page when a user clicks on the app in the center, the user can: 1) learn about the app; 2) visit the app's website; 3) read the app's privacy policy and terms of use; 4) set the audience for posts the app makes to Facebook Timeline on the user's behalf; 5) see the categories of 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)

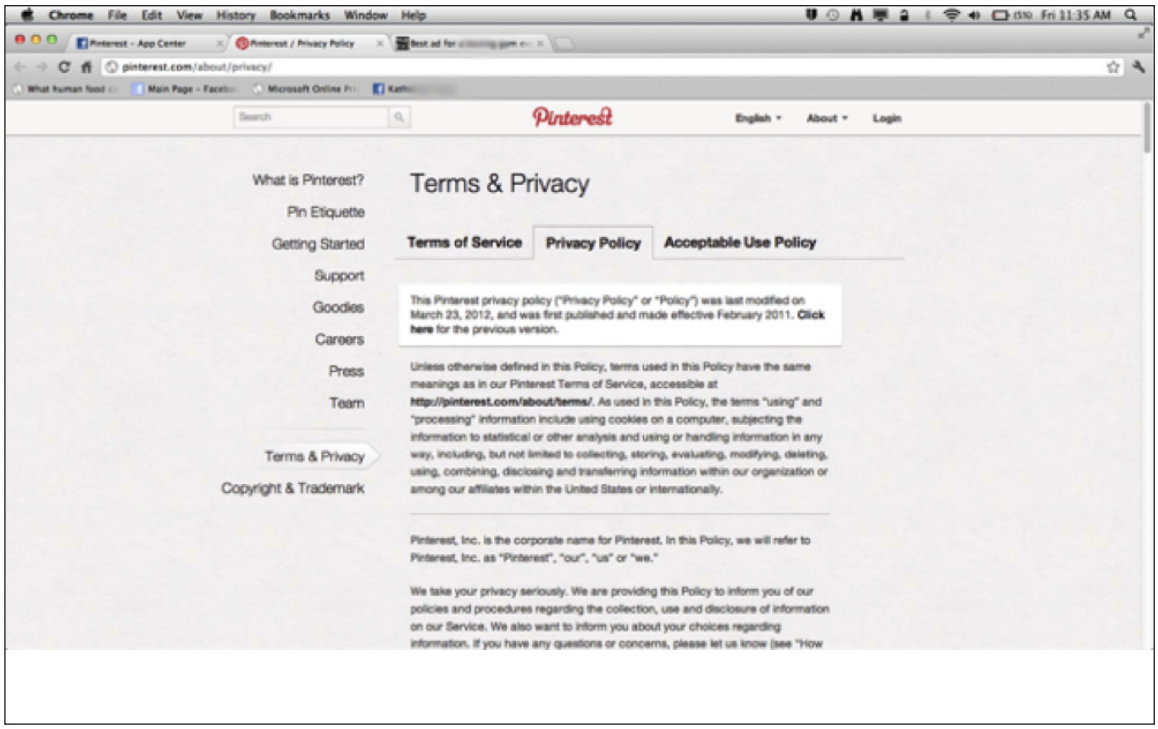
(audience control before adding app)

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

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



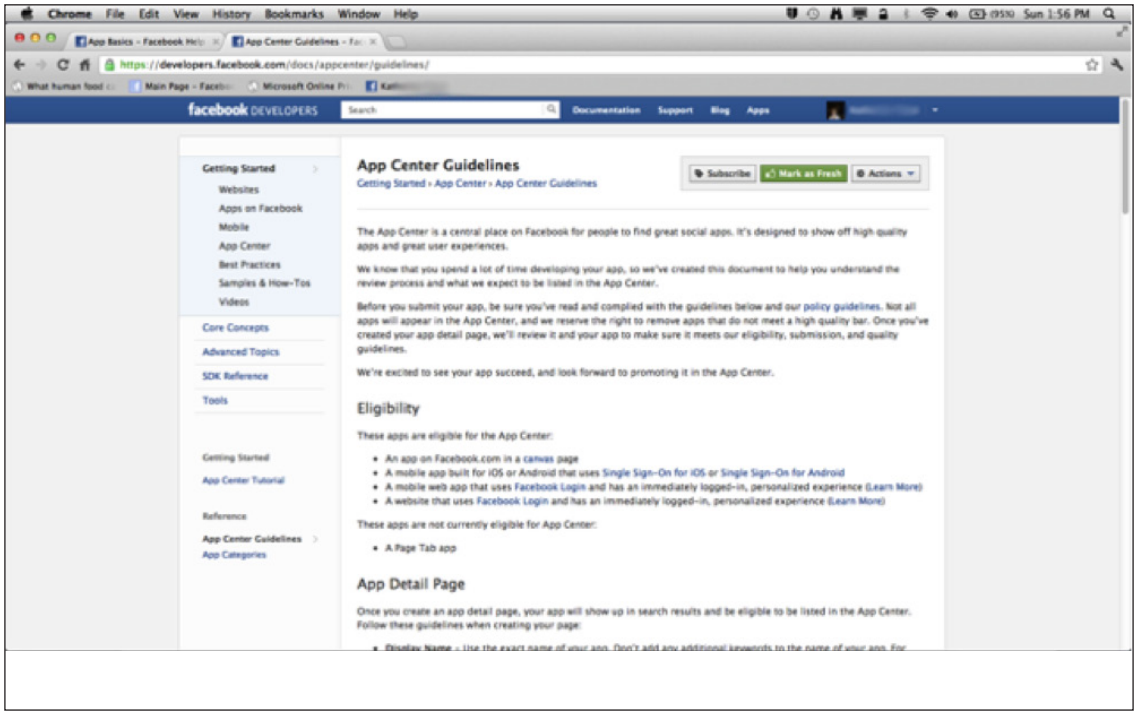
(report form)



(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/.

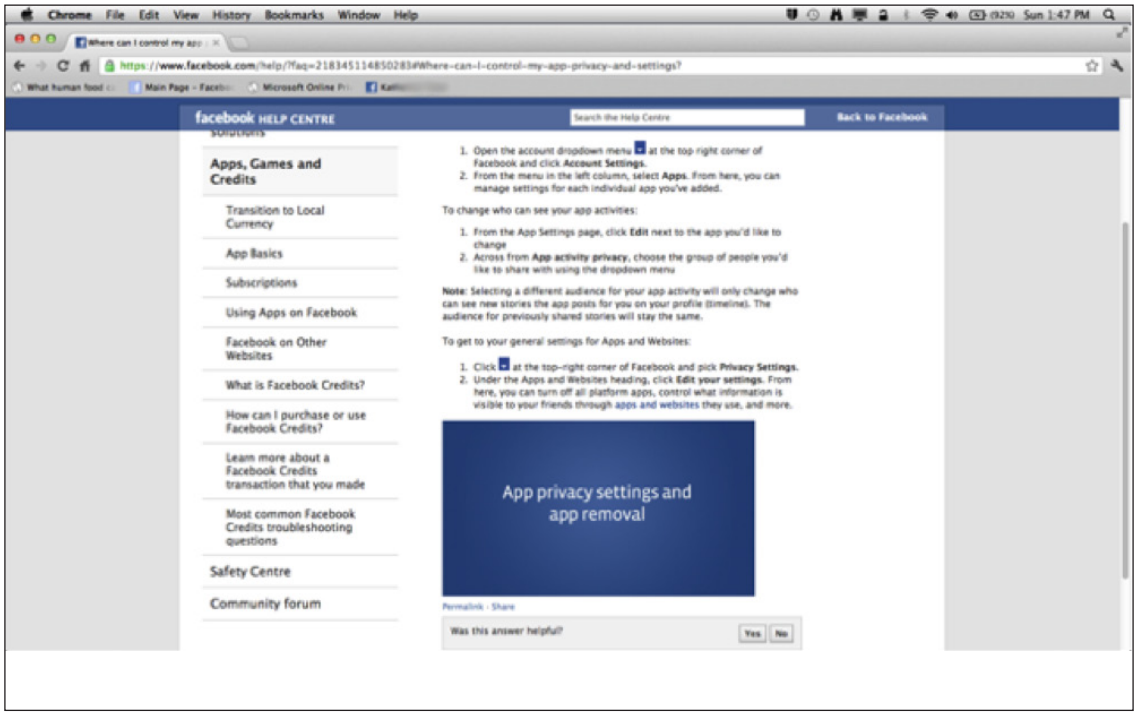
See screenshot below:



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.

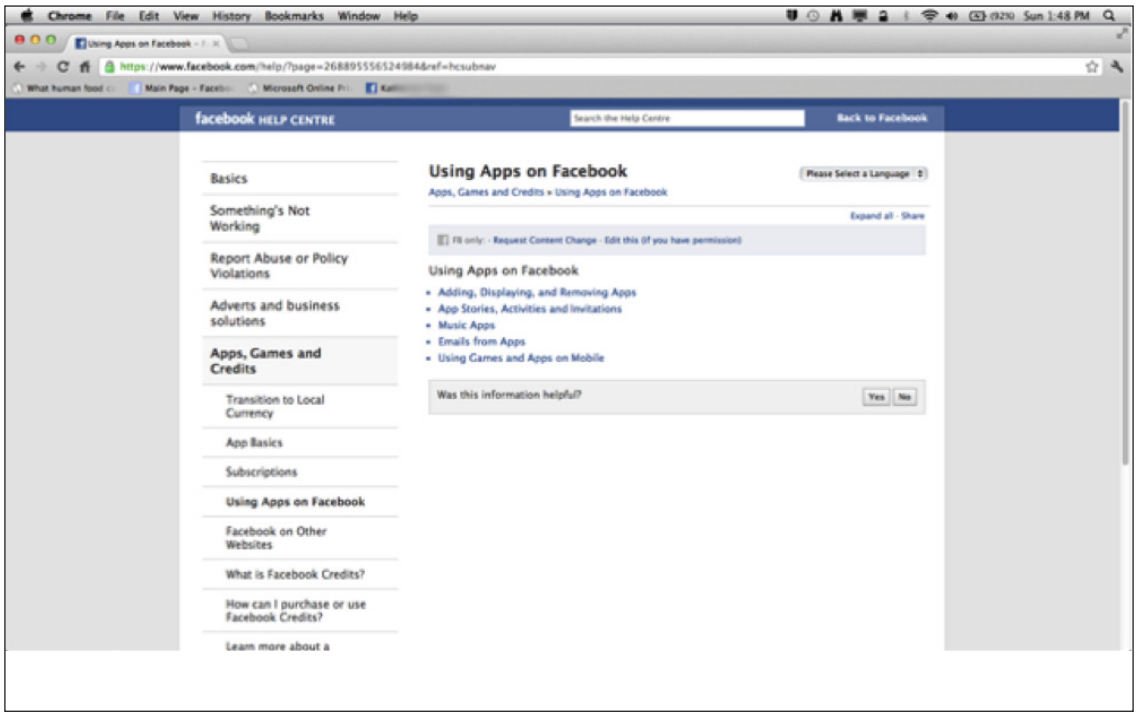
Another part of the user experience of apps on Facebook is the accessibility of information about how to find and use app privacy settings. FB-I provides easy to find information in its Help Center about where users can control their settings. See https://www.facebook.com/help/?faq=218345114850283#Where-can-I-control-my-app-privacy-and-settings.

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=268895556524984&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.

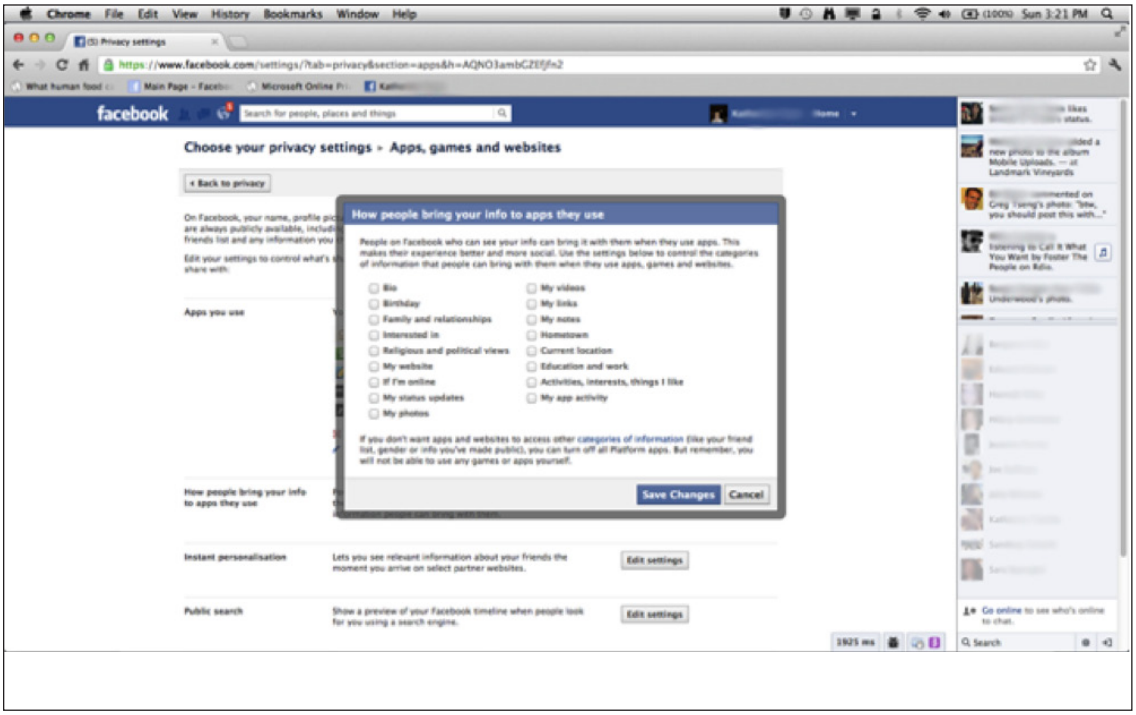
7.3 Tools for Monitoring Developer Compliance

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.

7.4 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. See Section 2.6.

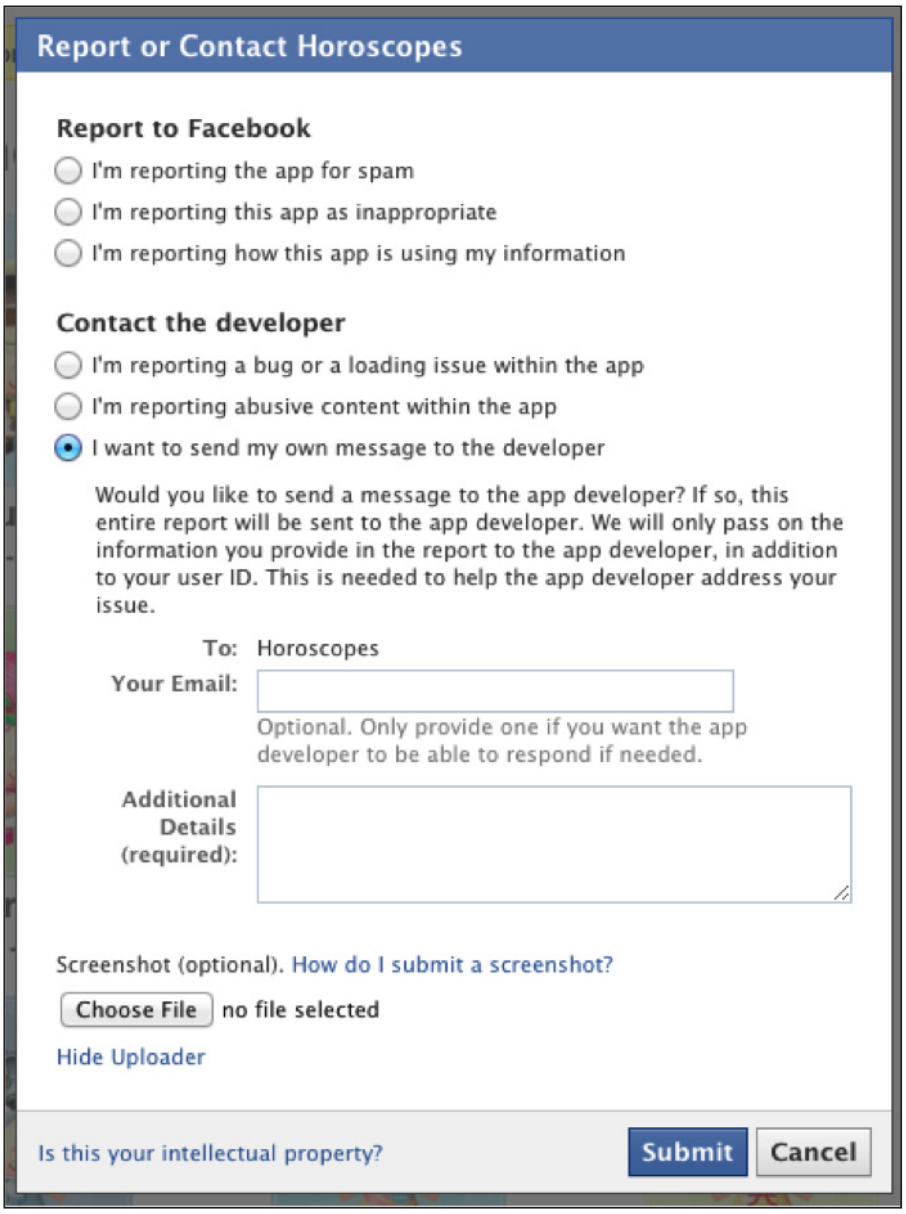
7.5 Reporting Apps

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.

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.

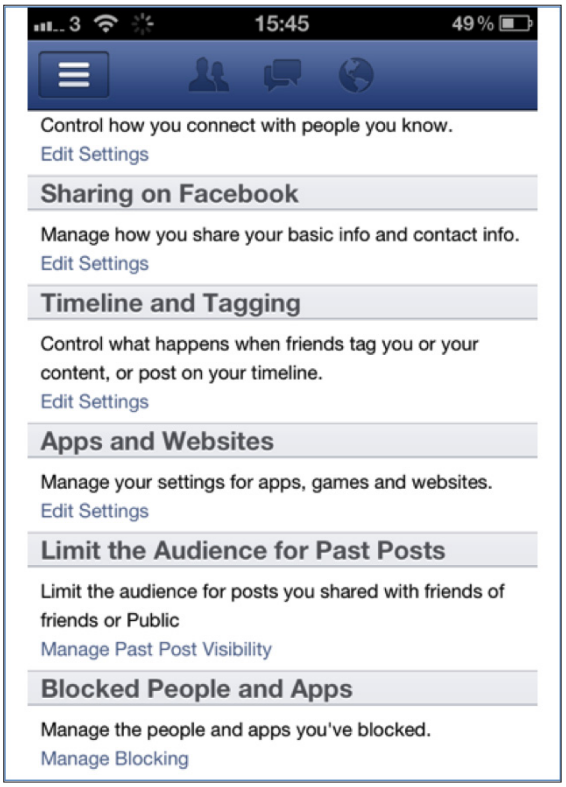
FB-I has also provided a direct means for a user to contact the developer of an app. See screenshots below.

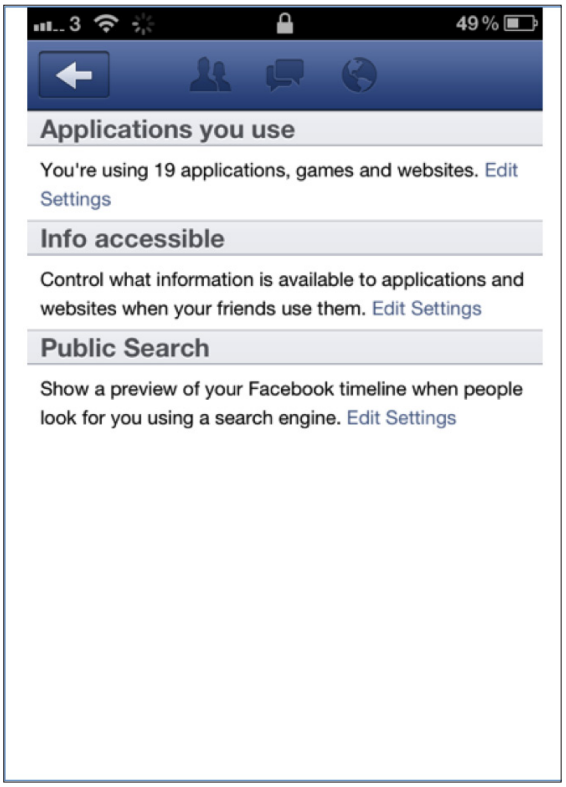


There are report link for apps on Canvas (facebook.com), in GDP (permissions dialogue box), and in App Center.

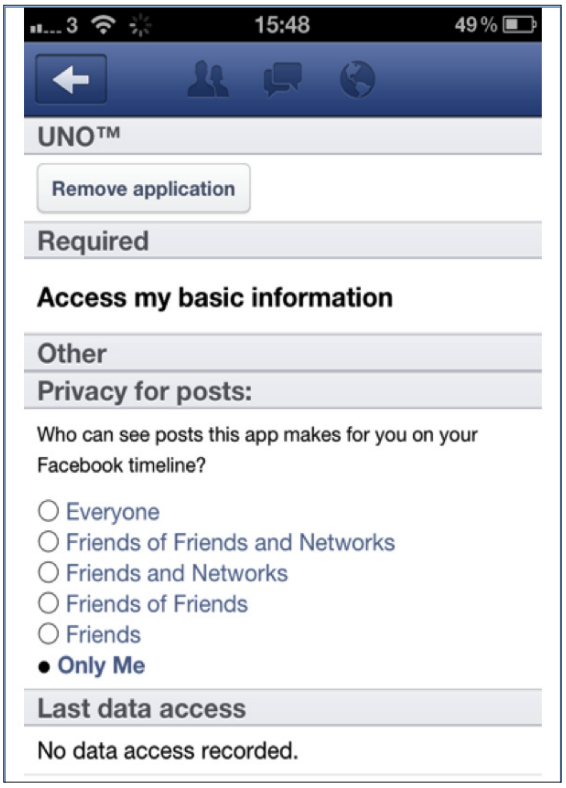
7.6 Mobile App Platform

The DPC indicated that Facebook Platform for Mobile would be examined in more detail in July 2012. The mobile environment is distinct from the web environment and presents opportunities for innovative ways to engage with and educate users, as their attention is typically focused on a much smaller screen, for shorter but often more frequent periods of time. Currently, FB-I offers users on Facebook's mobile web site many of the same basic controls that are available to users, via interfaces that are specially designed for the small screen that characterizes the mobile environment. See screenshots below:

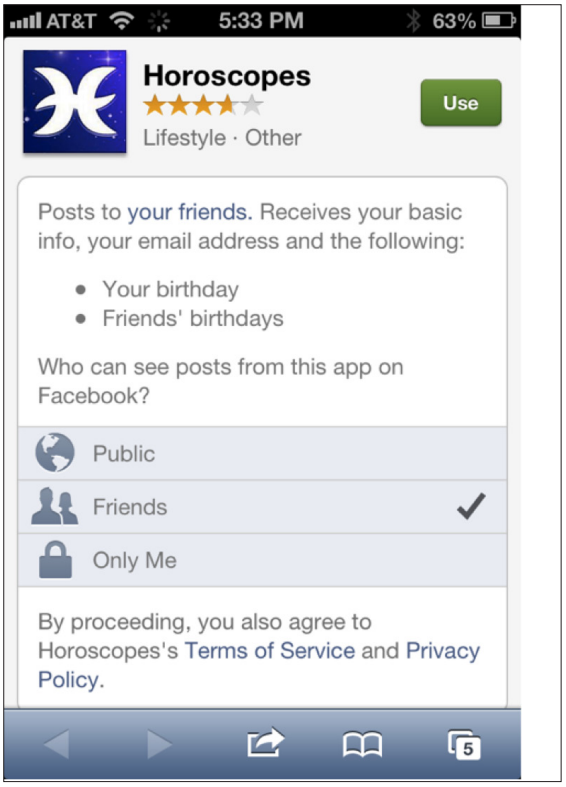


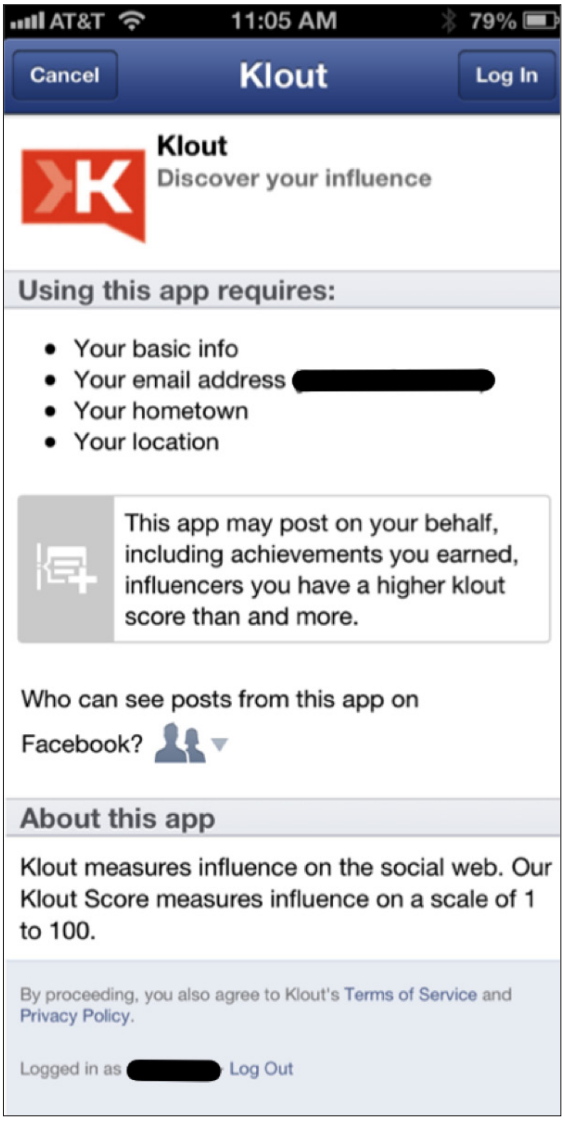


Users can access setting for a specific app on mobile. See screenshot below.



Apps on mobile contain the GDP dialog box. See screenshot below.





Native iOS apps also display a permissions screen when used within the Facebook app. See screenshot below.

7.7 Instant Personalization on Platform

Approximately two years ago, Facebook introduced Instant Personalization, a program offering Facebook users an instantly personalized experience on several third-party sites. The program was designed to highlight the benefits of a social and personalized experience on the web. To that end, Facebook chose a select number of partners that demonstrated that they could provide the kind of innovative and new experience that Facebook wanted. These partners signed special agreements with Facebook designed to protect users' data. Users who landed on one of the Instant Personalization sites see a bar across the top of the site that says the website is using Facebook information to provide a personalized experience. When the user lands on the site, Facebook passes the user's basic information (name, profile photos, cover photos, gender, networks, user name, user id, and anything the user has chosen to make public) to the site. Users are given an opportunity to opt out right away, and the partner site is obligated under its agreement to promptly delete the user's data if the user makes that choice. Users can also opt out of all Instant Personalization integrations with one click through their privacy settings.

FB-I's Data Use Policy contains a detailed section on Instant Personalization. See https://www.facebook.com/about/privacy/your-info-on-other#instantpersonal.

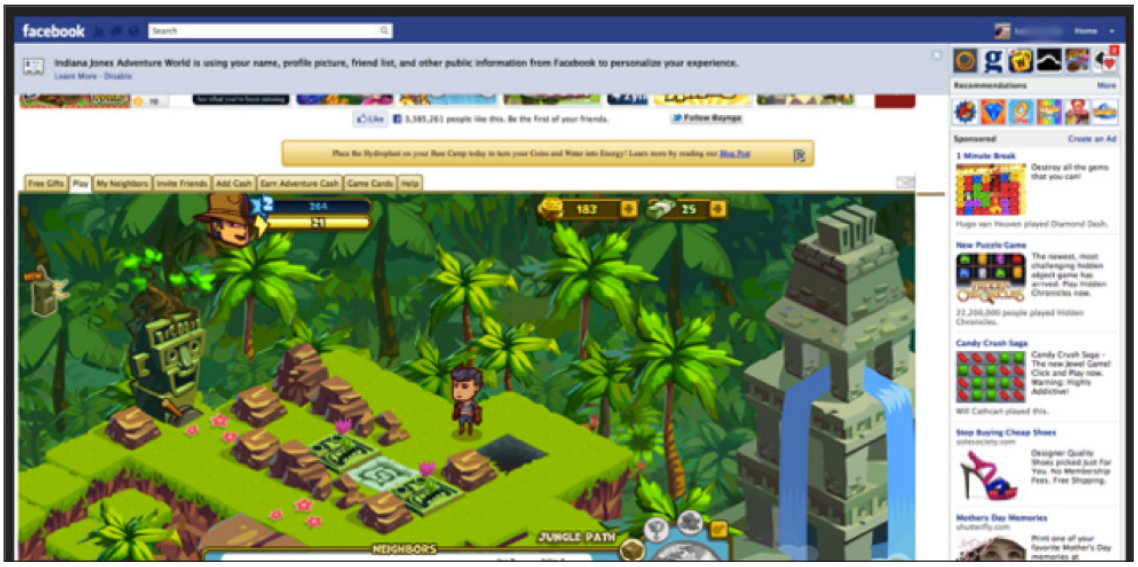
In July, Facebook introduced Instant Personalization on Facebook.com with a number of its most popular social game developers. Facebook has separate agreements in place with these developers, which include requirements analogous to those agreed to with the partners who integrated Instant Personilization into their web sites.

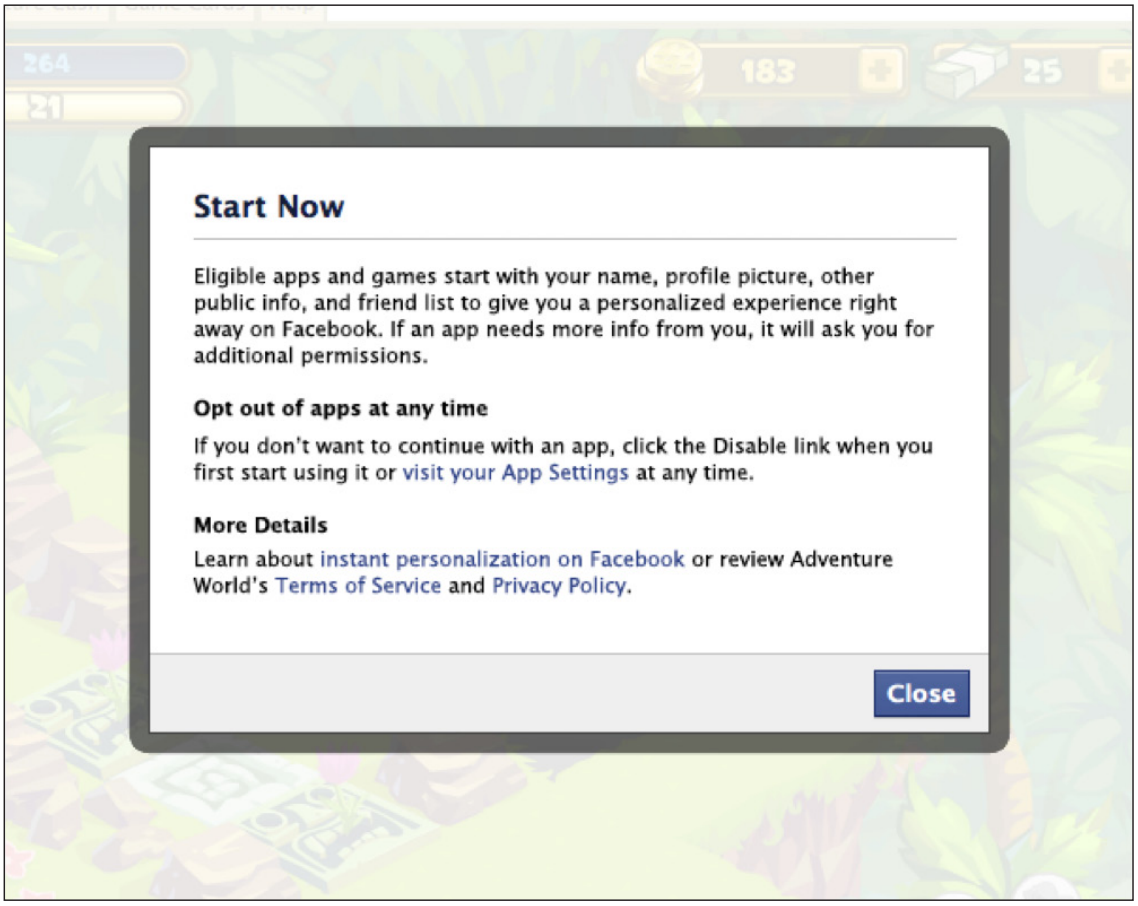
Instant Personalization on Facebook.com works in the following manner:

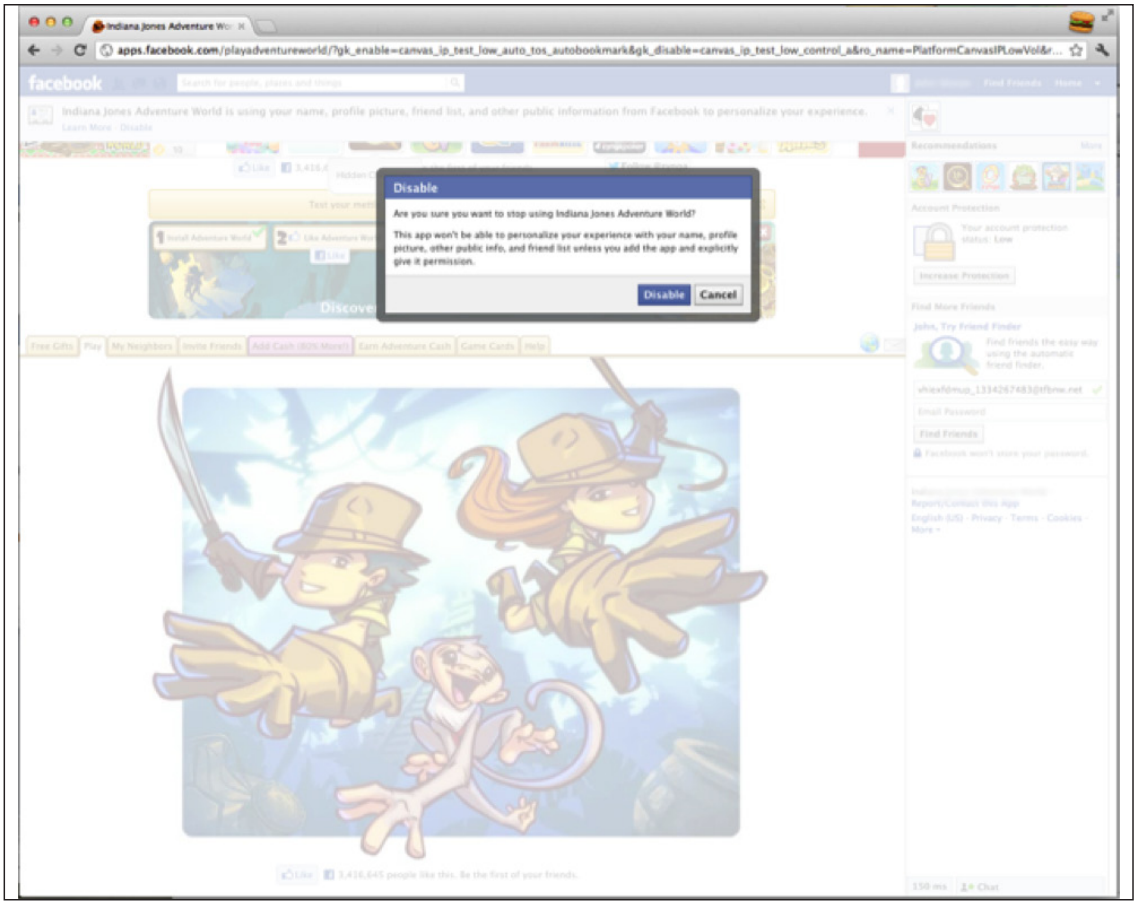
When a user lands on the app on Facebook, the app receives the user's basic information – name, profile picture and friend list – and information the user has set to public. At the top of the app, a banner is displayed, telling the user that the app is using this information to personalize the user's experience. Also displayed are the links "learn more" and "disable". If the user clicks "learn more", a pop-up appears giving the user additional information about the instant personalization experience, including links to the app's privacy policy and terms of service. If the user clicks "disable", a pop-up appears confirming the user's choice to disable the experience. If the user chooses to disable the app, the developer is required under its agreement with Facebook to promptly delete the information it received as a result of the Instant Personalization integration.

Apps are given only minimal, already-public information at launch. If they want more, they have to ask separately and expressly, which is clearer to users and creates a disincentive against asking for extra data or permissions.

Below are screenshots of the user experience:



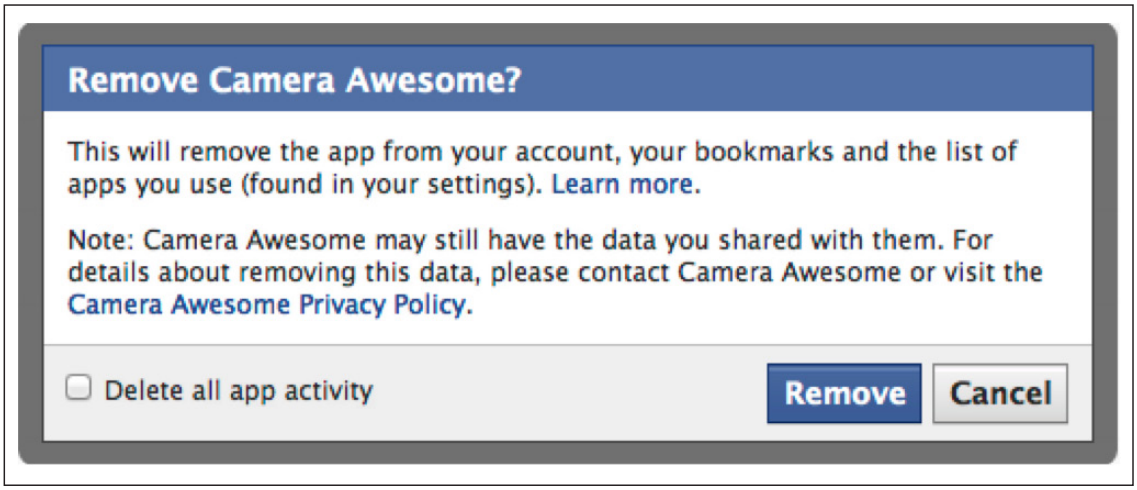




If the user clicks disable, he or she is taken back to the page he or she was on before landing on the app..

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.



Chapter 8 – Disclosure to Third Parties

In the Report of Audit, the DPC concluded that Facebook "adopts what we would consider to be an appropriate approach in dealing with such requests. It has ensured that requests are examined and considered by appropriately trained staff with restrictions in place within FB-I to ensure their confidential treatment. Each request is examined by virtue of the legal authority of the requesting law enforcement agency and the nature of the personal data sought. We are satisfied on the basis of our examination that requests which do not have an appropriate legal basis, seek content data or are too broad are refused. As outlined in its privacy policy, FB-I does release personal data in these circumstances when it has formed a good faith belief that doing so is justifiable. This consideration is based on Sections 8(b) & 8(d) of the Acts."

The DPC "recommend[ed] a continuation and extension of the SPOC (Single Point of Contact) arrangement with law enforcement authorities;" that the "SPOC arrangement should be further strengthened by a requirement for all such requests to be signed-off on or validated by a designated officer of a senior rank and for this to be recordable in the request;" that "the standard form be further strengthened by requiring all requesting entities to fully complete the section as to why the requested user data is sought so as to ensure that FB-I when responding can form a good faith belief that such provision of data is necessary as required by its privacy policy"; and that Facebook "re-examine its privacy policy to ensure that the current information provided is consistent with its actual approach in this area."

Facebook has further developed and strengthened the SPOC arrangements with the UK and Irish authorities and has actively promoted possible SPOC arrangements with other countries. In particular, Facebook has conducted training and outreach with the UK SPOC authorities to reinforce the legal and operational requirements to properly submit law enforcement requests to Facebook, including the importance of signed requests that provide details about the basis of

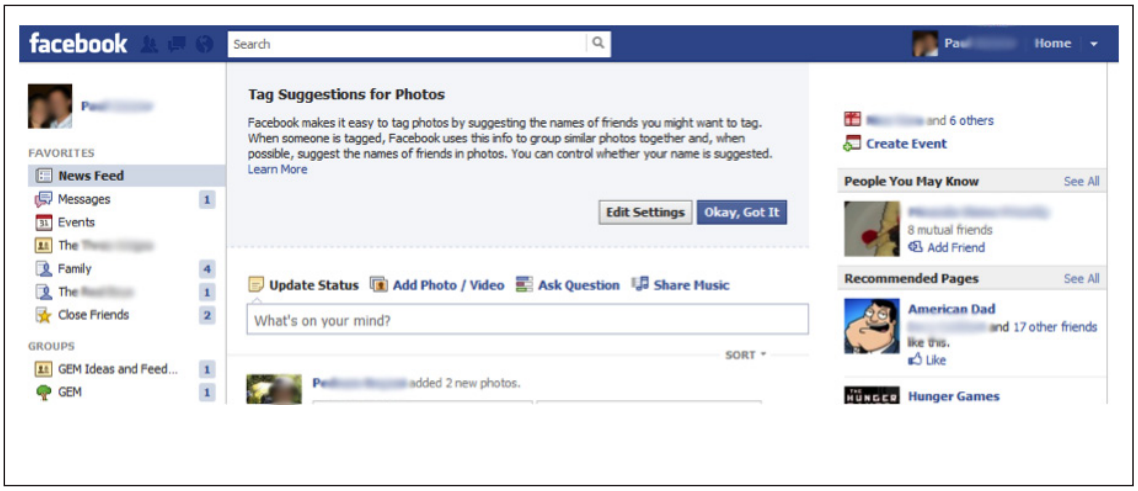
the request to ensure compliance with local law and Facebook's terms. Additionally, Facebook has encouraged law enforcement authorities throughout the EU to adopt a SPOC model in light of the mutual operational advantages of the SPOC system. These outreach efforts have been favorably received by law enforcement authorities in a number of countries and Facebook will continue to work to formalize processes to support the SPOC model where possible.

Chapter 9 – Facial Recognition/Tag Suggest

FB-I has now provided two sets of notice to users of its tag suggestions feature powered by facial recognition technology and has updated its Data Use Policy with a link to a more detailed description of tag suggestions. As the Report of Audit described, prior to the audit, FB-I had already voluntarily taken additional measures to give notice to users in the EU:

- Each user was given prominent notice of the new feature on her/ his FB-I home page. The notice appeared at least three times;
- The notice provided a link to further information on the feature, including how to disable it; and
- The then-current method of disabling the feature was modified to further simplify it.

Committed to representing best practices in this area, FB-I agreed to provide yet further notice to users. Between early January and July 2012, FB-I ran a banner on the user's homepage, which appeared at the top of the page when the user logged in. If the user interacted with the banner by selecting either option presented, then it disappeared for the user. If the user did not interact with it, then it appeared twice more for a total of three displays on the next successive log-ins. Before making a selection, more detail about how the feature works appeared behind a "Learn More" link. If the user clicked "Edit Settings", he would be taken to his privacy settings page where he could turn off the feature. See screenshot below:



FB-I has also Expanded notice of tag suggestions in its new Data Use Policy, which now states:

"We are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we've put together from the photos you've been tagged in. You can control whether we suggest that another user tag you in a photo using the How Tags Work settings."

The "How Tags Work" link goes directly to the privacy settings where the user can turn off tag suggestions.

After the Article 29 Working Party issued its recent Opinion on biometrics, the DPC indicated to FB-I the expectation that it would comply with the Opinion's recommendations. FB-I has temporarily stopped creating facial templates for users joining Facebook after July 1, 2012, while it decides on its approach to the Opinion's recommendations.

Chapter 10 – Data Security

There have been no substantial changes to the core Information Security Controls, which were deemed to be adequate during the December 2011 audit by the DPC. However, Facebook was in the processes of making considerable changes to how employee access to user data was managed, which was reviewed in detail in July.

Facebook has implemented a permission model that relies on an employee's role in the organization, as dictated by the Human Resources Management system. In addition to changing how permissions are granted and revoked, Facebook spent a significant amount of time building a system that provides granular access to a user's data. Access is granted to a specific employee, for a specific user, within a specific tool, based on a request initiated by the user. The new access method is known as "token-based access". Migration to the token-based access is ongoing – at the present time, all inbound requests serviced by operations teams are fully migrated to the token-based access model, and tokens will continue to be implemented across other workflows throughout the next 12 months

In addition to the core infrastructure security controls and the new data access controls, Facebook has also made significant progress in their monitoring capabilities. In December, basic data abuse detective capabilities existed and have been further improved to detect new avenues of potential abuse. The biggest change since December is a new a tool Facebook built to detect general security breaches using clustering and anomaly detection across all systems in the infrastructure. This new system goes beyond detecting known types of attacks or abuse, and looks at historical behavior of an account to determine unusual behaviors that could indicate a compromise. This system will continue to be developed, introducing new detection capabilities and operational procedures to respond to potential incidents.

Chapter 11 – Deletion of Accounts

Although many types of data have shorter retention periods, FB-I retains some user data for the life of the account. It's important that this information is completely deleted or otherwise deidentified upon account deletion. Where possible, FB-I prefers actual deletion to deidentification or other techniques. At FB-I's scale, direct deletion is not possible in some situations, and any deletion must be able to deal with a wide variety of distributed system challenges. FB-I thus set out to design account deletion in a way that is reliable and consistent despite this challenges. Because these challenges vary across types of storage, our solutions also vary by storage system.

11.1 User Databases

Most of the data users see on Facebook are stored and retrieved from our user databases. These are MySQL databases, where we leverage the traditional strengths of relational databases, including fast inserts, deletes, and indexed queries. Because these queries are efficient, we can walk through all of their content and delete it within a short period of time (typically between a few hours and a few days). Users have a home database where their core account information lives, and there are thousands of databases where they may also have content (e.g., a comment on a friends post will typically live on their friend's home database). One advantage of our user databases is that we've largely unified our data model over the last several years, building on a graph-like model of objects and assocs (edges) rather than tables with custom, per-product schemas.

11.1.1 Deletion Framework

Ultimately, this user database based account deletion had five goals:

1. Reliable. Delete all of the expected data and none of the unexpected data.
2. Restartable. Databases go down, machines hang, power fails. Deletion of an account involves deleting thousands of rows across thousands of different databases over minutes, hours, or days. If an account deletion is interrupted, it must be able to restart and successfully continue deletion.
3. Recoverable. If we discover an account was deleted in error shortly after it was deleted, we must be able to quickly and correctly recover the data. At FB-I's scale, recovering from traditional tape-style backups, while possible, is extremely painful and error-prone. Still, we limit our retention of the backups to ensure we do not hold user identifiable data more than 90 days after account deletion completes.
4. Rerunable. If we later discover a class of data that was missed in previous deletions, we need to be able to efficiently re-delete all previously-deleted accounts to clean up this newly-discovered data.
5. Reusable. Minimize the amount of code required per data element and ensure that we don't have one-off deletion code scattered across our codebase.

To meet these challenges, we built a deletion framework that centralizes conre functionality in a small number of rarely-changing components, gracefully retries deletion until it succeeds, keeps efficient, temporary, online backups, and has a test framework to verify correctness.

11.1.2 Migrations

The deletion framework relies upon being able to efficiently find data associated with a user starting from their user id. Historically, not all user data could be queried efficiently in this direction. For example, before Timeline's Activity Log was introduced, we never displayed a user's comment outside the post they commented on. Thus, we only needed to efficiently query from post to comment and comment to user, not user to comment. In order to reliably delete comments, we started writing an assoc from the user to their comments upon creation, then went through and backfilled this assoc for the 700 billion comments that existed on the site before this change. We've conducted similar migrations to enable efficient deletion of other types of data.

11.1.2 User Databases Deletion Timeline

Day 0: User requests permanent account deletion.
Day 14: Account deletion begins if not canceled by user in preceding 14 days.
Day 28: Deletion framework backups expire (assuming deletion completed in 1 day)
Day 104: Tape-style database backups expire (90 days after deletion began)

11.2 Hive

Hive is an open-source, SQL-like query layer built on top the Apache Hadoop framework for distributed map-reduce computing. Hive is the storage and offline analysis layer for all of FB-I's log data (multiple petabytes of data). Unlike the user databases, Hive does not have efficient row-based insert and delete, nor is data indexed by user. As a result, we cannot delete a user's log entries at account deletion time. Instead, we must to rely upon deidentification of data well before the account is deleted. This deidentification process completes within 90 days of the logs being generated to ensure that we do not hold identified data for deleted accounts in Hive beyond 90 days.

This inability to perform efficient, per-user queries is also why FB-I cannot today offer download of stored log data in response to subject access requests or in its user-facing DYI tools.

All logs in Hive have a specified retention period, and logs retained beyond 90 days have configuration that specifies where personal data lives in the logs. The deidentifiation process depends on this configuration, but also has built-in logic to find other personal data, such as the authenticated user's User ID embedded in a URL.

11.2.1 Deidentification

We use the term deidentification rather than anonymisation because we think it more accurately reflects what is being accomplished. Anonymisation and reidentification are areas of active research, and we cannot be 100% confident that deidentified data is truly completely anonymous to the degree it could be released into the public domain for research. Instead, our goal with deidentification is to remove all of the identifiers that we normally use in analysing this data, as well as any user-generated content and any other identifiers we can find. We apply the same safeguards to deidentified data as to the original data. For a deleted account, we have no reasonable way to identify which log entries correspond to that account versus some other account, thus we are unable to use this data for anything other than aggregate.

The original logs may include a variety of personal data and identifiers, including user_id, IP address, email address, datr cookies and even some user generated content. We have committed to deidentifying this log data within 90 days of account deletion.

By default, deidentification all identifiers and user-generated content are deleted from the logs. Two data fields have special handling: User IDs and the datr cookie in impression logs.

User IDs. Because we use logs older than 90 days for product improvement and other analysis, we cannot simply delete the user id. Additionally, because we perform longitudinal analysis of accounts over time, hashing the user id with a rotating secret will not work. Instead, we assign each User ID a corresponding Replacement ID (rid) that is constant for the life of the account. This mapping is stored in the user databases where the deletion framework ensures deletion during account deletion. This rid is not anonymous or deidentified until a user deletes their account.

The datr cookie. We also need to perform some per-browser analysis on logs older than 90 days. The datr cookie is our unique browser identifier. However, we do not need to perform long-term longitudinal analysis on this data, so we are able to hash the datr cookie combined with a secret that changes every ten days. Once the old secret is overwritten with the new secret, we are no longer able to find records based on a datr cookie. At that point, we consider the field deidentified.

As the logs near 90 days in age, we generate a rewritten copy to remove the vast majority of user identifiers and user-generated content. The only two identifiers that are left are the rid and the datr cookie hashed with the rotating secret. On the 90th day, we delete the original logs.

At this point, the logs at rest are in a deidentified state, which allows data scientists to perform some work without ever tying it back to an identified user. For undeleted accounts, we can use the rid to recover the original user_id. We use this when we need to use historical log data to train a model, which then affects the behavior of the site for that user. No such recovery is possible for deleted accounts.

This entire approach avoids needing to rewrite petabytes of data each time a user deletes their account. It also supports the goals of data minimisation by completely removing from Hive an entire class of personal data within 90 days (e.g., IP addresses, email addresses, and user-generated content).

11.2.1 Deidentification Timeline

Day 0: Activity on the site.
Day 10: Logged out social plugin impressions are deleted.
Ongoing: Logs reaching their retention limit are deleted.
Day 70: The deidentified copy of logs is generated.
Day 90: Original logs with personal data are deleted.
2 years: Any remaining ad click log data is deleted.

11.2 Other data stores

FB-I operates a few other specialised backend data stores. The two most interesting such stores are Titan, which is built on HBase and stores private messages, and Haystack, which is a custom space-efficient large-blob store used to store photos and private message attachements. It's

important that these data stores have the same properties of reliable deletion and rapid recovery from unintended deletions when discovered quickly. In both cases, this is implemented by flagging a record as deleted so that it is hidden from the site immediately, then purging the deleted data periodically. To further ensure our ability to recover photos that were unintentionally deleted, the first compaction over an object does not actually purge it unless sufficient time has passed. In no case, however, does this process take more than 90 days to completely purge the data.

Titan's use of shared message attachments is the last area of special requirements. When a user sends a private message to a friend on Facebook, each user ends up with an independent copy of the message body except any attachments. The attachment is actually stored in Haystack as a binary large object. Unlike the user databases where traditionally relational database features are available (e.g., transactions and locks), each HBase cell in Titan is completely independent. This makes a reference counting implementation far more complicated and error-prone. Thus we take a simpler approach. Each attachment is encrypted with a unique per-message, per-attachment key. This key is only stored in the sender's and each recipient's copy of the message. As each user deletes their copy of the message, they delete their copy of the encryption key. Once the last remaining user deletes their copy, FB-I is no longer able to decrypt the stored attachment. The encrypted attachment's metadata does not include any information about the sender or the recipients of the attachment. This results in some storage inefficiency (these attachments could otherwise be deleted to free space), but the benefits in reduced complexity and increased reliability are far more important. If the storage later becomes a problem, we will likely be able to identify orphaned encrypted attachments and delete even the encrypted data.

Chapter 12 – Business Contact Importer

The DPC sought to ensure that FB-I adhered to a zero-tolerance policy with respect to complaints received by individuals in the EU who were sent emails from Page administrators without having consented to the receipt of such emails. The DPC noted that FB-I already provided numerous protections around its business contact importer product to minimize the risk that EU individuals would receive emails from Page administrators. These measures included: 1) blocking all major EU domains; 2) requiring administrators to check a box affirming that they have consent to send the emails; and 3) prominently displaying a message that alerts Page administrators to the requirement that they comply with all applicable laws, including European laws.

FB-I currently blocks a dynamic list of over 300 internet domains, which is far over-inclusive and thus significantly reduces the risk that any Page emails will be received by individuals in the EU.

The DPC also advised that any addresses a Page administrator removed from its imported contacts should not be used for friend-finding purposes. In fact, currently, FB-I does not store any of a Page administrator's uploaded contacts and does not use any of such contacts for friend-finding purposes.

And finally, the DPC noted that it had received a complaint from an indiviudal who had received an SMS invitation whereby the opt-out mechanism did not work. FB-I disabled SMS invitations until it was confident any problem was resolved.

Chapter 13 – Tagging

The DPC examined the complaint by the group Europe v. Facebook, in which the complainant argued that FB-I was in breach of data protection law because users do not provide consent to be tagged. The DPC recommended, and FB-I agreed, that FB-I consider whether there were any additional controls that FB-I could offer and whether an "opt out" of tagging altogether would be feasible. FB-I did consider these questions. FB-I reviewed all of the current tagging controls that it offers. Tagging is an integral feature of the Facebook service – and one that FB-I has designed to be privacy protective by enabling a user to know when others are referring to him or her within the Facebook service and enabling him or her to take action if he or she prefers not to be mentioned.

Tagging is a core functionality of the Facebook service. Users have numerous controls over the tool, including the ability to review tags before they appear on a user's timeline, to un-tag photos, to review tags other users have added to the user's posts, and to control who can see posts the user has been tagged in on their own timeline.

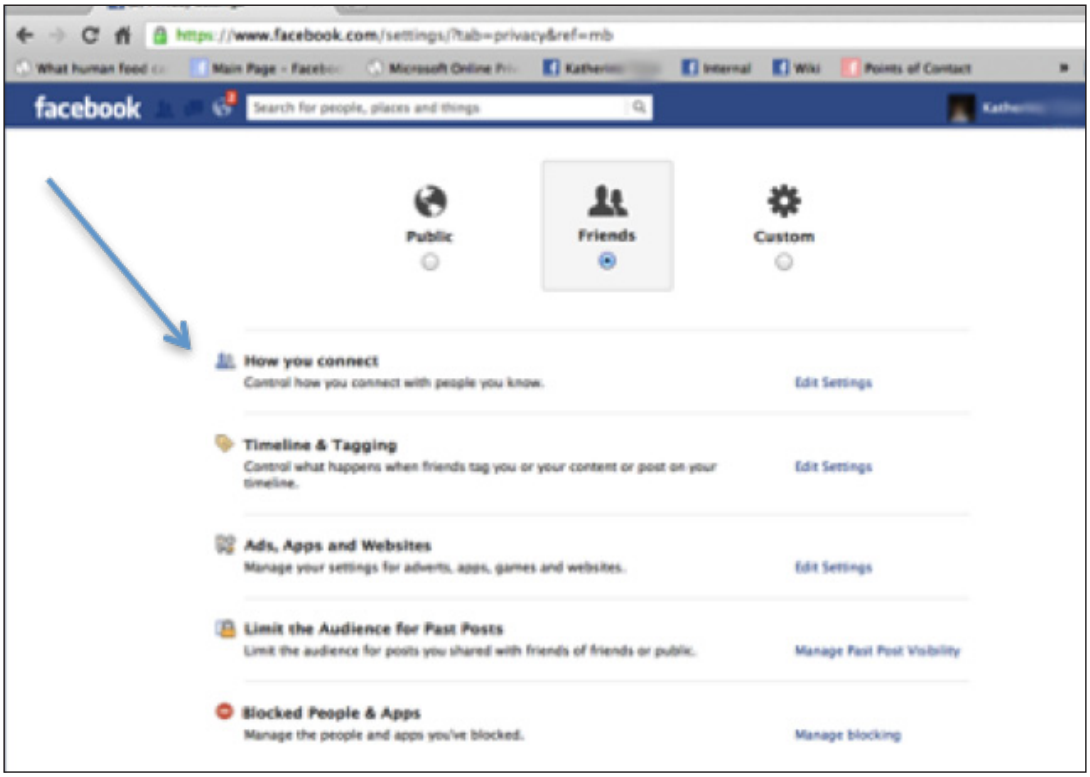
13.1 Consent

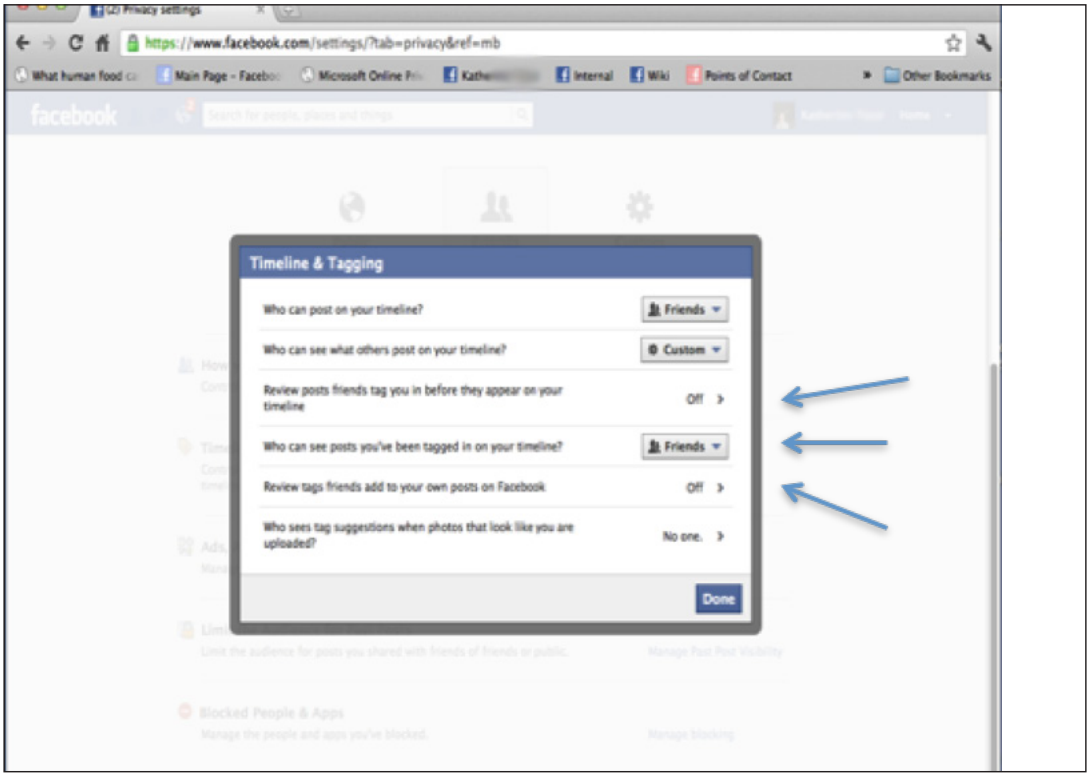
Facebook users agree to the Statement of Rights and Responsibilties and the Data Use Policy when they register for an account. The Data Use Policy contains a section about tagging. See below and https://www.facebook.com/about/privacy/your-info-on-fb#friendsshare.

> Links and Tags
>
> Anyone can add a link to a story. Links are references to something on the Internet; anything from a website to a Page or timeline on Facebook. For example, if you are writing a story, you might include a link to a blog you are referencing or a link to the blogger's Facebook timeline. If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see.
>
> A tag is a special type of link to someone's timeline that suggests that the tagged person add your story to their timeline. In cases where the tagged person isn't included in the audience of the story, it will add them so they can see it. Anyone can tag you in anything. Once you are tagged, you and your friends will be able to see it (such as in News Feed or in search).
>
> You can choose whether a story you've been tagged in appears on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can always remove it from your timeline.
>
> If you do not want someone to tag you, we encourage you to reach out to them and give them that feedback. If that does not work, you can block them. This will prevent them from tagging you going forward.
>
> If you are tagged in a private space (such as a message or a group) only the people who can see the private space can see the tag. Similarly, it you are tagged in a comment, only the people who can see the comment can see the tag.

13.2 Control

FB-I also offers users significant control over tagging. Tagging is to a significant degree pro-privacy – it is the main way users learn that photos in which they appear and content in which they are mentioned have been posted to Facebook and thereby made available for others to see. Users are notified each time they are tagged, at which time users can view the content and un-tag themselves if they want. Once un-tagged, the content is not hyperlinked to the user's profile/ timeline. Furthermore, users can choose to preview the tagged content and give approval before such content appears on their own timeline; they can choose who can see tags on their timelines; and they can review tags that others add to their posts on Facebook. See screenshots below.





13.3 Tagging as an Integral Product Feature

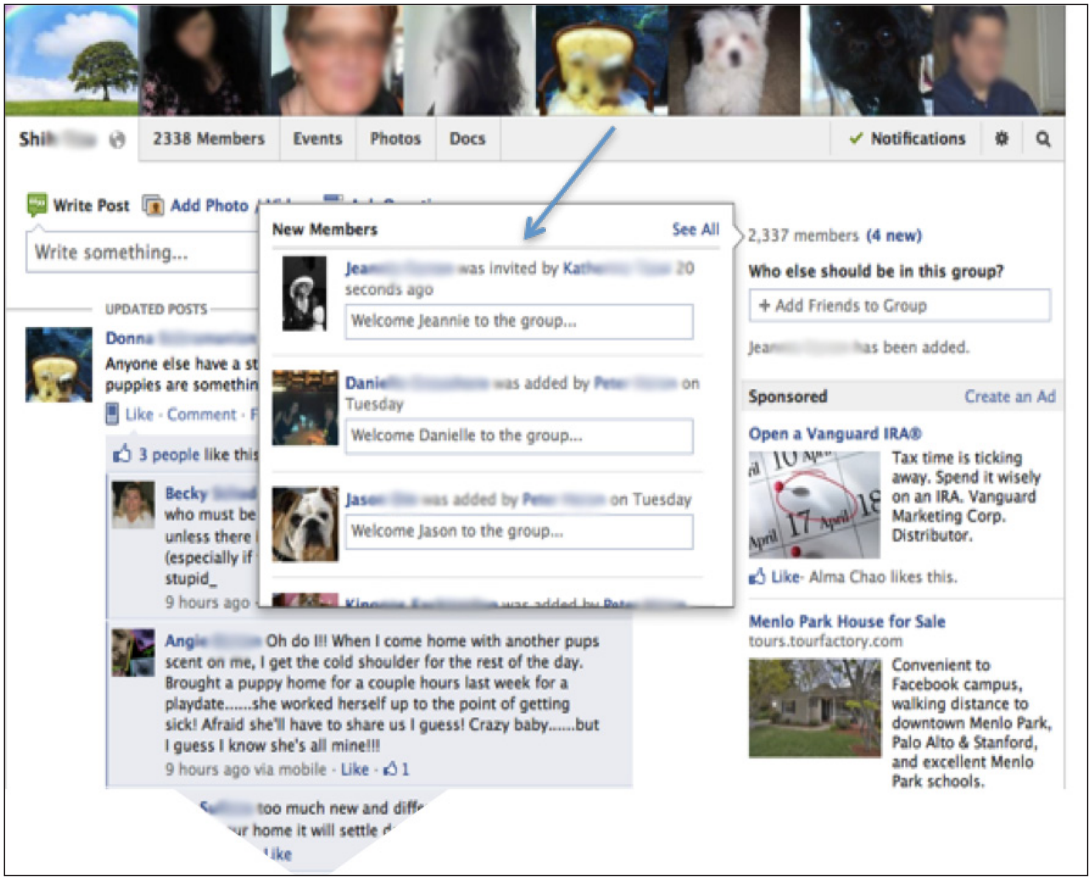
Tagging is core activity on Facebook and has been positively received by Facebook users. Tagging is an important tool for connecting, sharing, and communicating on Facebook. Tagging has emerged on Facebook as a short-hand way of sharing something with a specific person or people, along with the wider audience the user's content is visible to. With users having an average of over 100 friends, it is increasingly difficult to make sure that any one particular person is aware of content a user has posted. Because users receive notifications of tags, users are more likely to see content that others want them to see.

Furthermore, on the Internet in general, there is no easy way for people to learn when someone has commented about them, uploaded a photo that includes them, or created other content that includes descriptions of them. And even when people do become aware of such content, there is often no way for them to learn the identity of the author or request that content be modified, corrected, or deleted. Facebook users, on the other hand, have much greater awareness and control. They receive notifications when they have been tagged, and they have the ability to un-tag themselves. Tagging enables users to get informed immediately when someone mentions them in a post or a photo. It gives users more control, since they can react positively, express their discomfort and ask for the removal of the content if they wish, or simply respond to a post in which they are mentioned.

As tagging has expanded, FB-I has been sensitive to those users who may want more control over the process. Thus, FB-I offers users: 1) notice of tags; 2) the ability to pre-approve tags before they appear on their timelines; 3) the ability to un-tag; 4) the ability to simply block the tag from appearing on the user's own timeline; and, furthermore, the ability to completely delete the "un-tag". Furthermore, if a user feels in any way harassed by unwanted tags, the user can block the person, which will prevent that person from being able to tag him or her. FB-I believes that it has struck the right balance in terms of product development and user control.

13.4 Groups

In the Report of Audit, the DPC recommended that FB-I give users more control over deciding whether to join Groups. In response, FB-I changed the way users add their friends to Groups. Previously, any user could add a friend to a Group, and the story that would go into the newsfeed of their friends would be that User A added User B to Group C. The DPC expressed the concern that, to members of and visitors to Group C, it might appear that User B had taken an affirmative step to become a member. Now, User A invites User B to Group C, and the story that appears in the newsfeeds of their friends is that User A invited User B to join Group C. Until User B visits Group C and has the opportunity to leave the Group, to members of and visitors to Group C, it only appears that User B was invited to the Group. In this way, an inference cannot be drawn that User B has taken an affirmative step to join Group C simply because User B was invited. See screenshot below:



Chapter 14 – Posting on Others' Profiles/Timelines

The group Europe v. Facebook raised the complaint that Facebook users who posted on other users' timelines did not know the audience for their post. The DPC indicated an understanding of FB-I's position that it has trained users to understand the privacy model on Facebook: users control the visibility of their own timelines. Whenever a user posts on another user's timeline, the user whose timeline it is controls the visibility of the post. Although the DPC found this position largely reasonable, the DPC suggested that FB-I could compromise and display an approximate number of people to whom the post would be visible.

The DPC also suggested that because users can retroactively change the visibility of posts on their timelines, FB-I could message all users who posted on a timeline when the visibility setting was changed (presumably to something more open).

FB-I considered both suggestions carefully and concluded that neither could be implemented in a user-friendly way that respected the privacy model of Facebook and the privacy of users.

It is important to FB-I that users understand that content they share may, in turn, be shared by others more broadly and, if it is content shared on another user's timeline, will be visible to an audience that may be as wide as "everyone". It is a simple model, and it encourages responsible sharing. Users have the most control over their own timeline. But when a user decides to post on another user's timeline, he or she does so understanding that he or she does not control the visibility of the post. Users who wish to communicate privately can use any one of Facebook's messaging products – messages, emails, or chat.

Furthermore, Facebook already offers users the ability to see the general audience of a user's post on his or her timeline, which means, users who wish to make a comment on that post can see the general audience of the comment, e.g., friends of friends of the user whose timeline it is.

Chapter 15 – Facebook Credits

The DPC recommended that FB-I make it clearer to users that FB-I was the data controller with respect to credits. In its Data Use Policy, FB-I tells users that it receives data about them when they purchase Facebook Credits or make other purchases through Facebook:

"We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook."

The Statement of Rights and Responsibilities lists FB-I as provider of the Facebook service, and states that "[i]f you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms." The Payment Terms state that such terms are between EU residents and FB-I.

Chapter 16 – Compliance Management/Governance

In the Report of Audit, the DPC stated: "[I]t is clear that senior staff in Dublin play a substantial role in the handling of user data by FB-I. We have acknowledged that meeting the compliance responsibilities for the day to day handling of user data in an environment such as FB-I is challenging in and of itself given the scale of the data involved. However, we can also acknowledge that this Report has demonstrated that FB-I has made significant progress over the past number of months in meeting its access, retention, minimisation, deletion, disclosure, international data transfer and fair processing responsibilities under the Data Protection Acts."

16.1 Data Transfer

FB-I has processing agreements in place with all entities to which it transfers data for processing on its behalf. The agreements provide for specific and limited processing of user data in service of FB-I's operations and have been prepared so as to meet the requirements of EU and Irish law.

16.2 Direct Marketing and Employee Training

During the audit, the DPC examined the area of FB-I's direct marketing activities focused on acquiring new business customers. The DPC noted that while this did not relate to the processing of user data, FB-I could generally improve by documenting procedures to ensure that data protection considerations are taken fully into account when direct marketing is undertaken either by or on behalf of FB-I.

FB-I has responded by conducting employee direct marketing training with a focus on EU laws. The training included new materials that have been created for the specific purpose of educating employees on EU laws.

Furthermore, all FB-I employees receive confidentiality and privacy training upon induction. In addition, and so as to further ingrain privacy into the FB-I's culture, staff from across numerous departments are obtaining the highly regarded information professional/ Europe certification from the International Association of Privacy Professionals.

16.3 Data Privacy/Product Review

In its Report of Audit, the DPC noted that with the Facebook Inc.'s agreement with the FTC in place, there would be significant improvements to and oversight of the privacy review process at the Facebook U.S. headquarters. However, the DPC was interested primarily in how FB-I would ensure compliance with Irish data protection law requirements. The DPC acknowledged that FB-I has recently brought about a large number of data protection improvements for the users for which it is responsible. The DPC also noted that additionally the policy casework team provides day-to-day expression of the commitment to handling privacy complaints from or about individual users. The DPC recommended, however, that FB-I take further measures to build up a data protection compliance team in Dublin and to put in place a more comprehensive mechanism, resourced as appropriate, for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law.

To this end, FB-I has appointed a senior lawyer as Head of Data Protection in Dublin, who has formed a data protection compliance team with members from legal, policy, platform, law enforcement, security, engineering, and user operations in Dublin, as well as ad hoc members located elsewhere in the EU, and the United States. The team's focus will be on ensuring data protection compliance in all areas of the operation of Facebook. The team will work closely with counterparts in entities responsible for processing user data. See Appendix 2 – Data Protection Compliance Team.

The FB-I data protection compliance team will work closely with counterpart teams in Facebook, Inc. Specifically, the Head of Data Protection will be involved in all product review prior to the launch of products in the EU, and will be responsible for ensuring that products and features comply with Irish data protection law prior to launch in the EU. Facebook, Inc., has established a product review structure that is led by its two Chief Privacy Officers (one for Product and the other for Policy). The Head of Data Protection will be part of the product review team.

APPENDIX 1 – FB-I Data Compliance Team

FB-I has appointed a Head of Data Protection, a senior lawyer whose responsibilities will be focus on ensuring Facebook Ireland and Facebook Inc. comply with Irish, European and global data protection and privacy. The Head of Data Protection will establish and manage a cross-functional and cross-disciplinary data protection and privacy compliance team in Dublin. The head of data protection will manage a team of regulatory lawyers, who will assist in: advising Facebook Ireland and Facebook Inc. on Irish, European, and global data protection and privacy laws; working with internal product, privacy, advertising and marketing, policy, and communications teams to ensure compliance with Irish, European and global data protection and privacy laws; training EMEA staff as needed on applicable European regulatory requirements; in managing European and global regulatory inquiries; collaborating with Facebook's International legal team on diverse legal issues facing international offices; and establishing and maintaining positive and cooperative working relationships with European data protection regulators, including FB-I's European regulator, the Irish Data Protection Commissioner.

FB-I's cross-functional compliance team will include members of each of the relevant departments in FB-I, each of whom will be acting under the supervision of the Head of Data Protection.

Members include:

Law Enforcement Response Team (LERT): This member will be responsible for keeping the head of data protection aware of all law enforcement request issues that raise data protection concern; training, in coordination with regulatory counsel, new LERT staff on data protection compliance; and liaising with U.S.-based LERT.

Payments: This member will be responsible for ensuring that payment systems and procedures are reviewed by regulatory counsel for data protection compliance.

Information Security (InfoSec): This member will be responsible for liaising with U.S.-based InfoSec to ensure the FB-I established policies and procedures relating to EU user data, including employee access, security, etc., are being adhered to.

User Operations: This team will include members from the privacy group, the authenticity group, and the abuse group. Members will be responsible for following established policies with respect to data-protection issues that are raised by users, including, subject access requests, and imposter/fake accounts.

Platform Operations: This member will ensure that data protection issues on platform are escalated to the regulatory counsel and will continue to work on systems and policies to give users easy avenues to report data protection complaints to FB-I and to improve FB-I's response.

Policy: This member will be responsible for responding to user complaints forwarded to FB-I from regulators and to some inquiries made directly by regulator.

Platform Policy: This member will be responsible for ensuring that platform policy is compliant with data protection law.