An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Facebook Ireland Ltd

Report of Audit

21 December 2011

Table of Contents

APPENDICES

Executive Summary

This is a report of an audit of Facebook-Ireland (FB-I) carried out by the Office of the Data Protection Commissioner of Ireland in the period October-December 2011. It builds on work carried out by other regulators, notably the Canadian Privacy Commissioner, the US Federal Trade Commission and the Nordic and German Data Protection Authorities. It includes consideration of a number of specific issues raised in complaints addressed to the Office by the "Europe-versus-Facebook" group, the Norwegian Consumer Council and by a number of individuals.

The audit was conducted with the full cooperation of FB–I. It found a positive approach and commitment on the part of FB-I to respecting the privacy rights of its users. Arising from the audit, FB-I has already committed to either implement, or to consider positively, further specific "best practice" improvements recommended by the audit team. A formal review of progress is planned in July 2012.

The audit was conducted by reference to the provisions of the Data Protection Acts, 1988 and 2003, which give effect to the European Union's Data Protection Directive 95/46/EC. Account was taken of guidance issued by the EU's Article 29 Working Party[1]. The audit team followed the standard audit methodology used by the Office[2].

Facebook is a platform for users to engage in social interactions of various kinds – making comments ("posts") on various issues, setting up groups, exchanging photographs and other personal material. It has some 800 million users, spread throughout the globe. FB-I is the entity with which users based outside the United States and Canada have a contractual relationship. FB-I is the "data controller" in respect of the personal data of these users.

As a "data controller", FB-I has to comply with the obligations set out in the law. The report summarises the audit team's conclusions on how FB-I gives effect to the basic principles of data protection law: that personal data should be collected "fairly"; that the individual should be given comprehensive information on how personal data will be used by FB-I; that the personal data processed by FB-I should not be excessive; that personal data should be held securely and deleted when no longer required for a legitimate purpose; and that each individual should have the right to access all personal data held by FB-I subject to limited exemptions.

In addition to examining FB-I's practices under standard data protection headings, the team also examined in detail the data protection aspects of some specific aspects of FB-I's operations, such as it's use of facial recognition technology for the "tagging" of individuals, the use of social plug-ins (the FB 'Like' button), the "Friends Finder" feature and the 3rd Party Applications ('Apps') operating on the FB platform.

In examining FB-I's practices and policies, it was necessary to examine its responsibilities in two distinct areas. The first is the extent to which it provides users with appropriate controls over the sharing of their information with other users and information on the use of such controls – including in relation to specific features such as "tagging". This also includes the rights of non-

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf
[2] http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf

users whose personal data might be captured by FB-I. Various recommendations have been made for "best practice" improvements in this area.

The second main area where we examined FB-I's practices and policies related to the extent to which FB-I uses personal data of users to target advertising to them. 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.

A key focus of the audit was the extent to which the "deal" could reasonably be described as meeting the requirements of fair collection and processing under the Data Protection Acts. While acknowledging that this is a matter of judgment – ultimately by Irish and European Courts – the general conclusion was that targeting advertisements based on interests disclosed by user's in the 'profile' information they provide on FB was legitimate. We also concluded that, by extension, information positively provided by users through 'Like' buttons etc could legitimately be used as part of the basic "deal" entered into between the user and FB-I. The legitimacy of such use is, in all cases, predicated on users being made fully aware, through transparent notices, that their personal data would be used in this manner to target advertisements to them. And any further use of personal data should only be possible on the basis of clear user consent. Various recommendations have also been made for general "best practice" improvements in this area.

The privacy governance structure within FB-I was also examined. The comprehensive settlement reached by the Federal Trade Commission (FTC) with Facebook and announced on 29 November 2011 should ensure that Facebook will adopt a rigorous approach to privacy and data protection issues for the next 20 years. The focus of the audit was on the possible changes needed to strengthen the capacity of FB-I to ensure compliance with the specific requirements of Irish and EU data protection law.

Progress on implementing the specific recommendations contained in the Report will be reviewed in July 2012. This will be part of the Office's continuing engagement with FB-I.

The Office would like to thank Dave O'Reilly of University College Dublin who provided invaluable assistance in examining a range of technical issues that arose in the audit. We would also like to thank the other regulators whose work we relied on, as detailed in various parts of the report. The responsibility for the content of the Report lies solely with us. On a personal note I wish to thank the other staff members in our Office who worked to very tight deadlines in the conduct and completion of this Report.

The recommendations in the Report do not carry an implication that FB-I's current practices are not in compliance with Irish data protection law. Neither do they represent formal decisions of the Commissioner on the complaints submitted to him as the Audit was led by me under the Commissioner's authority.

Gary Davis
Deputy Commissioner

List of Recommendations and Findings

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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	FB-I will work with the Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate.	End Q1 2012 and routinely thereafter
	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.	Agreed. Furthermore, FB-I has agreed to take the additional step of moving the links to the Data Use Policy and other policy documents, as well as the Help Centre, to the left side of the user's homepage. Presently the use of Credits is required only for games that monetise through virtual goods.	End February 2012
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	FB-I will clarify its data use policy to ensure full transparency.	By the end of Q1 2012

	transparent with users as to how they are targeted by advertisers		
	FB-I does not use data collected via social plug-ins for the purpose of targeted advertising	FB-I is taking steps to limit data collection from social plugins, is restricting access to such data and is moving to delete such data according to a retention schedule where collected.	Immediately and routinely thereafter (with the exception of retention for legal hold obligations)
	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	Agreed.	By the end of Q1 2012.
	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.	FB-I will enter into discussions with this Office in advance of any plans to introduce such functionality.	n/a
	The current policy of retaining ad-click data indefinitely is unacceptable.	FB-I will move immediately to a 2-year retention period which will be kept under review with a view to further reduction.	Review in July 2012
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	FB-I will fully comply with the right of access to personal data, as outlined in the schedule	In line with the schedule in relation to availability from the user's profile, their activity log and

	request within 40 days, in the absence of a statutory exemption	contained within the Access Section of the Report. It has additionally committed to a key transparency principle that users are entitled to have easy and effective access to their personal information.	the download tool. Data will be added to the various tools in phases, beginning in January 2012.
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.	FB-I will comply with this recommendation in an updated Data use Policy.	By the end of Q1 2012.
	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.	FB-I will phase in such transparency and control to users on a regular basis.	FB-I has agreed to begin working on the project during Q1 of 2012. FB-I has committed to showing demonstrable progress by our July 2012 review. This time-scale takes account of the size of the engineering task.
	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 recorded 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 recorded as being a member until	By the end of Q1 2012.

		s/he visits the group and will be given an easy method of leaving the group	
	Personal data collected must be deleted when the purpose for which it was collected has ceased	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	Immediate and ongoing, subject to any legal holds placed on the data by civil litigation or law enforcement. The continuing justification for these periods will be kept under continuous assessment and will be specifically re-assessed in our July 2012 review.

		receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin. 3. anonymise all search data on the site within six months 4. anonymise all ad click data after 2 years 5. significantly shorten the retention period for log-in information to a period which was agreed with this Office	
	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.	FB-I will provide additional information in a revised Data Use Policy	By the end of Q1 2012.
	We have confirmed that data entered on an incomplete registration is deleted after 30 days		
	Data held in relation to inactive or de-activated accounts must be subject to a retention policy	FB-I will work with this Office to identify an acceptable retention period	July 2012.
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.		
	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	Impression data received from social plugins will be anonymised within 10 days for logged-out and non-users and deleted within 90 days, and for logged-in users, the data will be aggregated and/or anonymised in 90 days.	Immediately and to be verified by this Office subject to any legal holds placed on the data by civil litigation
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	FB-I has recently changed its granular data permissions dialog box for apps, which was expected to be fully available on all applications in February 2012, to allow for contextual control over the audience that will see the user's activity on Facebook.	End-February 2012 and assessed again in July 2012
	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	FB-I has recently changed its granular data permissions dialog box for apps where users can choose the audience ("audience selector") for their app activity directly in the dialog box.	Assessed again in July 2012
	The privacy policy link to the third party app should be given more prominence within the application permissions	There is a "report app" link in every dialog box, which permits users to notify FB-I of any	End February 2012 and ongoing

	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.	issues regarding the app, including a missing or non-working privacy policy link. In addition, FB-I will further educate users on the importance of reading app privacy policies and is positively disposed to increasing the size of the link in the dialog box and will report back to this Office.	
	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.	FB-I will implement this recommendation and is urgently examining how to introduce this feature from a technical feasibility perspective.	FB-I's progress in implementing this recommendation will be explicitly examined on our review visit in July 2012.
	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 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	FB-I will positively examine alternative placements for the app privacy controls so that users have more control over these settings	FB-I will report back on this point to this Office in advance of July 2012.

	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.	FB-I will provide more messaging to developers highlighting its policy regarding sharing of authorization tokens. In addition, FB-I will commit to investigate technical solutions to reduce risk of abuse.	End of January 2012 in relation to notification to apps developers. Immediate assessment of issue identified with outcome/solution presented by end of Q1.
	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	FB-I has proactive auditing and automated tools designed not just to detect abuse by developers, but to prevent it in the first place and the findings of the audit will be used to further refine the tools.	Progress review in July 2012.

	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.		
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	FB-I is implementing these recommendations.	To be commenced by Facebook in January 2012 and reviewed in July 2012.

	the current information provided is consistent with its actual approach in this area.		
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.	First week January 2012 at the latest
	We have confirmed that the function used to delete the user's facial profile is invoked when the user disables "tag suggestions".		
Security	Many policies and procedures that are in	FB-I will continue to document policies	Newly documented policies and

	operation are not formally documented. This should be remedied.	and procedures as required to maintain consistency in security practices.	procedures to be reviewed in July 2012.
	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 will integrate user password resets by employees into our monitoring tools	End-January 2012
	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 is implementing a new access provisioning tool that will allow for more fine-grained control of access to user data.	We will thoroughly review the application and usage of the new token based tool in July 2012.
	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		

	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.		
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.)	FB-I had already devoted a substantial amount of engineering resources to progressing account deletion to an acceptable level and is committed to working towards the objectives outlined by this Office.	Review in July 2012
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.		
	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	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, which providers do not provide disclosures on security risks. FB-I will have further dialogue in order to	End of Q1 2012.

	users should nevertheless be made aware when choosing this option.	work towards reviewing alternatives for reducing risk and addressing them through education or changes in the product.	
	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.	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.	End of Q1 2012.
	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 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.	End of Q1 2012.
	We confirmed that passwords provided by users for the upload of contact lists for friend-		

	finding purposes are held securely and destroyed		
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.	FB-I will examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review	In advance of July 2012
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.	FB-I will examine the broader implications of the suggested approaches and having done so will engage further on this issue in the July 2012 review.	In advance of July 2012
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	FB-I will be adding information to this effect in the Data Use Policy and it is launching a privacy policy for its payments systems in approximately six months.	End of Q1 2012.

	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.		
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	We are satisfied that FB-I has appropriate and accessible means in place for users and non-uses 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	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	FB-I has implemented these recommendations and supplied the relevant documentation produced and training given to this Office.	Complete

	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.		
	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 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.	We will fully assess the improvements made in this regard in July 2012 and will expect that by that time FB-I will have in place the procedures, practices and the capacity to comprehensively meet its obligations in this area.

Chapter 1 – Introduction

Social Networking is a phenomenon by any standards. It is now taken for granted as a means of communication, expression and interaction by nearly 800 million people. Yet it only commenced in a real way as recently as 2004. In many respects it is therefore not surprising that social network providers, regulators and most importantly individuals have encountered difficulty in ensuring that privacy is fully addressed by social networks. Equally, it is accepted by all that close attention must be paid to social networks, and, in this case FB-I, because of the opportunity for so much sharing of content and information including by minors and the possibility that users will not fully understand how to control the visibility and transfer of such content and information.

While the EU Data Protection Directive[3] and the Irish Data Protection Acts[4] which transposed the Directive in Ireland could not have reasonably foreseen the development of such technology, the technology neutral nature of the provisions do provide a sound basis on which to assess social networking and specifically in this context FB-I's compliance with the law in this area.

An important point to make at the outset is that the Office of the Data Protection Commissioner is satisfied that it has jurisdiction over the personal data processing activities of FB-I based on it being established in Ireland. Helpfully this position is fully accepted by FB-I which maintains the position that it wishes to comply with Irish data protection law and by extension European data protection law based on its establishment in Ireland. The position of the Data Protection Commissioner should not however be interpreted as asserting sole jurisdiction over the activities of Facebook in the EU.

Facebook established its European headquarters in Dublin in 2008. The role and position of FB-I in relation to users outside of the USA and Canada was significantly enhanced in September 2010 when Facebook's Statement of Rights and Responsibilities[5] was amended to designate the contractual relationship for such users to be with FB-I and not Facebook Inc. Since 2008 the Office of the Data Protection Commissioner has maintained regular and ongoing contact with FB-I. Contacts have ranged from being briefed by FB-I in advance of certain product developments and launches, to being notified of selected changes to policies or terms and conditions which could potentially have privacy implications for Facebook users. In September 2010 in recognition of the necessity to raise awareness in relation to the requirements of EU Data Protection law, the Commissioner visited Facebook Inc HQ in Palo Alto, California and met with the company CEO and other senior executives with roles and responsibilities which could be influential in this area. Also, as is the norm for all organisations based in Ireland who seek guidance from the Office, FB-I was provided with advice and guidance by the Office on matters that might give rise to compliance issues under Irish and EU data protection law. In addition, the Office of the Data Protection Commissioner corresponded with FB-I in relation to any formal complaints received from users based outside the USA and Canada. We also noted following the change in the Statement of Rights and Responsibilities that citizens and data protection authorities of a number of EEA member states have brought Facebook related issues to our attention for resolution with FB-I.

[3] Link to text of 95/46/EC
[4] Link to Law Reform Commission consolidation
[5] Link to Statement of Rights and Responsibilities

As a natural progression to these frequent contacts and given the increased importance of FB-I within the Facebook group of companies, the Office of the Data Protection Commissioner indicated to FB-I at the beginning of 2011 its intention to carry out a general audit of its data protection practices, under the powers conferred by Section 10 (1A) of the Data Protection Acts.

In August 2011, an Austrian-based advocacy group - **'Europe versus Facebook' -** submitted 16 detailed complaints to the Office in relation to various aspects of FB-I's privacy policy and practices. In September 2011, 'Europe versus Facebook' submitted an additional 6 complaints. There is a brief overview summary of the complaints in Appendix 2. As the investigation of these complaints would likely have involved addressing many of the issues that would arise in the audit, the Office decided to run the two processes in parallel, i.e. conduct the audit and the initial assessment of the complaints within the same timeframe. We also received three complaints from the Norwegian Consumer Council[6] which dealt with third party applications, the Facebook privacy policy and a question of jurisdiction. A summary of these complaints is also attached at Appendix 2. The complaints which were well researched provided a specific evidence based focus to the audit in a number of areas.

As referenced in the subject matter piece on access in the report, the complaint submitted by "Europe v. Facebook" in relation to access generated significant interest which resulted in FB-I receiving in excess of 40,000 subject access requests within a matter of weeks. This in turn led to this Office receiving approx. 600 access request complaints.

In accordance with normal practice, the complaints received from Europe-v-Facebook and the Norwegian Consumer Council were referred to FB-I with a request that all complaints be responded to prior to the commencement of the audit. FB-I complied with this request, comprehensively responding to the initial complaints and the additional complaints within the timelines set on each occasion.

As outlined in its 'Data Protection Audit Resource'[7] it is the practice of the Office of the Data Protection Commissioner to treat audit reports as confidential documents. They are therefore not published, though the audited organisation is free to do so. Exceptionally on this occasion in advance of the audit, FB-I and the Office agreed that the final report would be published in full at the conclusion of the process.

In the conduct of this audit we also sought, in so far as is possible, to take account of investigations carried out by other privacy regulators in Canada, the Nordic Countries and Germany who had also recently examined aspects of Facebook's privacy and data protection practices. The report also takes into account the Article 29 Working Party Opinion 5/2009 on Online Social Networking[8] with the recommendations made drawing upon the valuable work in that Opinion. Finally, the Technology Sub-Group of the Article 29 Working Party produced a compendium of issues of concern to members which greatly assisted the conduct of the audit.

The Office would like to thank the UCD Centre for Cybersecurity & Cybercrime Investigation part of the UCD School of Computer Science and Informatics which following a request from this Office

[6] Link to complaint of Norwegian Consumer Council
[7] http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf
[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

provided, on a pro bono basis, an experienced staff member, Mr. Dave O'Reilly to assist in the conduct of this audit from a technical perspective. Mr. O'Reilly's input and assistance was of enormous benefit throughout the conduct of the on-site element of the audit and the subsequent detailed analysis of the information received and sought from FB-I during the audit. Mr. O'Reilly's Technical Report and Analysis can be found at Appendix 1 of this report.

Chapter 2 - Audit

2.1 Introduction

The on-site element of the audit took place over six days 25-26 October, 16-18 November and 14 December 2011. The stated purpose of the audit was to examine FB-I's compliance with the principles set out in the Data Protection Acts and in the EU Data Protection Directive a data controller established within this jurisdiction. An issue which has arisen in the complaints, which are assessed throughout this report, is the extent of the data protection responsibility which FB-I has as a social network provider for the content posted by individual members. Under Irish law where an individual uses Facebook for purely social and personal purposes to interact with friends etc they are considered to be doing so in a private capacity with no consequent individual data controller responsibility. This so-called domestic exemption means for instance that there are no fair processing obligations that arise for an individual user when posting information about other individuals on their Facebook page. The Article 29 Working Party Opinion 5/2009 on online social networking also recognised this distinction. The Opinion also specifies circumstances whereby the activities of a user of a Social Network Service (SNS) are not covered by the 'household exemption'. If an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exemption does not apply.

It is clear in the light of the Opinion, that FB-I continues to have a number of separate responsibilities which are examined throughout this report.

A broad outline of the focus for the audit was provided to FB-I in advance. In addition, it had been indicated that the audit would be conducted taking account of the eight principles of data protection, namely:

- Fair obtaining and processing of personal data
- Ensuring data is kept for one or more specified, explicit and lawful purposes
- Disclosure / further processing / transfer of data to a Third Country
- Ensuring the data processed is adequate, relevant and not excessive
- Ensuring the data processed is accurate, complete and up-to-date
- Data Retention: ensuring personal data is kept for no longer than necessary
- Safety & Security of Data
- Access to personal data upon request

Full cooperation was received from FB-I during the audit. All access sought to data and information was provided. FB-I also provided full and ongoing access to all relevant staff in Dublin via the incoming Director of Operations in Dublin, Ms. Sonia Flynn who was present throughout the audit to assist in its conduct. Additionally FB-I arranged for senior staff members with relevant experience from Facebook Inc to attend. These included Joe Sullivan, Chief Security Officer; Arturo Bejar, Director, Engineering; Michael Podobnik, Manager, Information Security; Scott Renfro, Software Engineer, Security Engineering; and Travis Bright, Product Manager, Site Integrity and Support Engineering.

2.2 Overview of Structure and Functions

The initial two days of the audit focused on gathering a full understanding of the structure of Facebook and in particular FB-I and the data held in relation to users. In addition to Ireland and

the USA, Facebook has international offices in Singapore and Hyderabad, as well as to local Facebook offices located across the globe.

The focus on the structure of FB-I and the data it holds arises in part from the increased responsibility assigned to FB-I since September 2010 for all users outside of the USA and Canada. For our Office, the focus is on establishing that there is a substantive presence in Dublin which does have a responsibility for the user data of Facebook members.

FB-I provided the Inspection Team with a copy of a model contract entitled "Data Transfer and Processing Agreement" between FB-I Limited and Facebook Inc in which FB-I Limited was referred to as the data exporter and Facebook Inc the data importer. The Team was also provided with a copy of a data hosting services agreement between FB-I Limited and Facebook Inc as the service provider. Relevant sub-processing agreements with Facebook India & Facebook Singapore (these Offices perform essentially user operations functions in their regions) were also examined. All the relevant contracts which were effective from September 2010 were considered to be in order.

FB-I has some 400 staff working out of its Dublin office. A detailed overview of the functions performed by FB-I is included at Appendix 3. An overview of the role and functions of the Facebook Offices throughout Europe is attached at Appendix 4. During the audit we sought and received copies of appropriate data processing contracts entered into by FB-I as data controller and Facebook UK, Sweden, Italy, Germany, France and the Netherlands.

FB-I staff operate across the following teams:

- Developer Relations
- Site Reliability Operations
- User Operations
- Risk Operations
- Network Operations
- Database Operations
- Legal
- Law Enforcement Response
- Public Policy
- Payment Operations
- Platform Operations
- Online Sales Operations
- Inside Sales Operations
- Advertising Operations
- Marketing
- Finance
- Learning & Development
- Human Resources
- Staffing
- Real Estate & Facilities
- Physical Security

In line with normal practice for an audit, a number of areas were selected for a detailed examination. The specific areas were not provided to FB-I in advance of the audit but were chosen on the days in question. Certain of the detailed examinations conducted are outlined in the relevant subject matter areas and where there was no specific subject matter focus they are detailed individually below.

2.3 Site Reliability, Network Operations and Database Operations

All three of these areas are staffed by a common support team of Operations Engineers who provide front line management and monitor Facebook's core server network and database system infrastructure. Systems are monitored by the FB-I Operations Engineers who cover two roster shifts with a mirror team of counterparts in Palo Alto covering the other two roster shifts, with a one hour overlap between teams allocated to each shift swap-over. Data is accessed on remote servers via an encrypted channel. All of these servers are currently situated in data centres in the United States. Recently plans were announced to build a new data centre in Sweden.

2.4 User Operations

FB-I described User Operations as being one of the largest teams in Dublin. The stated goal of this multi-lingual team is to promote a safe environment for users by enforcing Facebook's Data Use Policy and Statement of Rights and Responsibilities. The User Operations Division responds to alleged breaches of terms of service, as well as user feedback and suggestions about the product. Such breaches could include intellectual property breaches, hacked accounts, inappropriate content, fake profiles, private impersonation of individuals and cyber-bullying.

A physical inspection was undertaken of several work stations in User Operations to assess the nature of the tasks being performed and view the level of personal data being processed. The User Operations Team used two integrated tools – Content Review Tool (CRT) and Ticket Processing System (TPS) – that are used to review content which could be infringing Facebook Terms of Use, assess all reports received and to correspond with the individuals who had reported the issues.

The Intellectual Property Team deals with about 60 trademark and defamation claims per day. We examined the TPS. It was noted that the Irish Team handled all queries and complaints from Ireland and the UK as well as any complaints received in German, Spanish, Italian, French, Dutch or Turkish. For all other languages, FB-I indicated that the correspondence would be translated in Dublin by a native speaker, then reviewed by experienced Intellectual Property reps from Palo Alto and Austin, TX. The Palo Alto and Austin IP reps, working in tandem with the User Operations Dublin language reps, take action on the claim until successful resolution.

The Inspection Team viewed a copyright complaint from a user in Germany where one user alleged that a photograph of himself which he indicated was his intellectual property was being used without his permission by another user. In a case like this, following an examination of the report, the Team member may decide to simply remove the photograph so that the user may no longer use/publish the photograph.

The Team then visited another area in User Operations where fake profiles, private impersonations and complaints alleging cyber-bullying are investigated by FB-I. Several thousand reports are received each day from users. Cyber-bullying reports are dealt with within 48 hours. If

any reports are received with reference to potential suicide, these reports are prioritised immediately. FB-I also stated that it uses a proactive monitoring tool which seeks to identify issues around child abuse. The Team noted the large amount of data on each screen regarding the individual being investigated, including the amount of friends they had amassed over time and how many of these friends had sent friend invites in comparison to invites issued by the individual. Many of the fields were presented in percentages and visually depicted using graphics similar to pie charts. The data protection issues arising are dealt with in the subject matter pieces on the right of access to personal data and retention.

The Inspection Team also visited the team dealing with fake accounts. Complaints or reports may take the form of one user reporting that another user of a Facebook account is false or not a real person. An email may be sent to the alleged fake user asking them to provide some proof of identity. It was outlined that some reports are not genuine – it may be a case of one person simply disliking another and making a complaint. However, it was indicated that if FB-I collected the proof that the account was fake, the account would be removed, although FB-I offers the removed account holder an opportunity to appeal.

We also examined a number of privacy related queries. One was from a French user who sought the removal of her deceased father's account. She sought full removal as opposed to memorialising (which is a status that FB-I will place an account if it is verifiably notified that an account holder has passed away). This request was acted upon once the requester was in a position to supply verification of the death of her father. However, FB-I did confirm in line with its standard policy that it could not provide any information on the account itself.

Another case related to a French user who as the Mother of a 14 year old in France sought the deletion of her daughter's account as she was unhappy with the use her daughter was making of the account. It was explained to the mother that FB-I could not delete the account on her request and she was provided with extensive information on how to engage with her daughter in relation to her concerns.

Also examined was a complaint from a female user in Germany in relation to a fake account allegedly posted by a former boyfriend. The account in question was already removed by the time the complaint was received. The complainant sought IP address and other contact details for the poster of the fake profile but again FB-I pointed out that such information could only be provided by legitimate legal means such as a court order or via a relevant law enforcement authority relying upon a relevant legal basis. We noted from an examination of the various complaints that where supporting documentation was sought to verify identity that it was immediately deleted as part of the workflow once identity was proven.

2.5 Legal Division/Compliance

FB-I's Legal Division at present deals mainly with compliance and contracts, working with Facebook's global engineering and legal staff and outside counsel to ensure that all Facebook products and policies are developed in accordance with applicable European and Irish regulations, including data protection laws.

An examination was conducted of the input of FB-I to product development and risk assessment. This is now an issue which FB Inc is required under the terms of the settlement reached with the

FTC to devote particular attention and resources. While the settlement reached is with FB Inc it applies under its terms to FB-I also. As outlined later in this report it is the position of this Office that FB-I ensure it is adequately resourced to be in a position to meet its data protection responsibilities.

2.6 Public Policy Division

The Public Policy Division works with legislators and regulators to explain Facebook policies and to resolve complaints. The Division also handles media queries in relation to new Facebook developments and data subject access requests. It is currently developing a pan-European team drawn from locally based Facebook offices across Europe in order to give feedback on policy issues to FB-I. These employees based in local offices do not have access to Facebook member data.

2.7 Sales Operations

Online Sales Operations handle the management of advertising accounts which are mainly created through the self-serve advertising tool available on the Facebook website. A number of issues which arose during discussions with these Teams are dealt with in the subject matter areas on advertising and retention.

Inside Sales Operations also handle the management of advertising accounts with associated interaction with local offices (Facebook France, Facebook Germany, etc) and is responsible for bringing new business to Facebook through generating new sales leads. The data protection compliance of the process in place at the time of the audit is separately assessed in this report.

2.8 Real Estate

This Division manages the Europe and Middle Eastern (EMEA) region real estate portfolio providing support for the various offices located throughout the region.

2.9 Physical Security

This Division provides physical security support to all teams and offices in the EMEA region including access controls and security procedures and policies.

2.10 Finance

The Finance Division has a staff of 16 and manages the majority of business needs for all Facebook offices outside North America.

Activities include order to cash functions; assessing customer credit worthiness, reviewing FB-I Ad Insertion Orders for revenue compliance, all billing, vendor management, monthly financial reporting, compliance and payroll.

It was noted that another of Finance Division's listed functions is to "partner with ad sales and user centric teams on strategy, prioritization, system enhancements, performance reporting, sales compensation programs and resource planning".

It was confirmed that the Division has access to certain classes of member data for forward planning purposes. This access was examined in further detail during the audit and was found to be controlled and proportionate.

2.11 Human Resources/Learning & Development

The Human Resources Division manages all staff in the EMEA Region. Payroll is managed from Dublin with some local service providers contracted as data processors to issue FB-I payslips. The precise relationship between FB-I and the local offices throughout the EU was examined. It was clarified that each local Office acts as the employer of the employees based there and therefore acts as a data controller at least in relation to employee data.

Staff orientation for all staff in the EMEA Region is undertaken in FB-I. This Division also provides learning and development training/opportunities to all staff in the EMEA region.

All new recruits receive training on confidentiality and security as part of their orientation as well as signing an employee confidentiality agreement. The Team was provided with a copy of the slides on confidentiality and privacy as presented to new recruits. In addition, as part of employee ongoing learning and development, employees must complete an online training module on confidentiality and privacy every year. FB-I stated that all employees must complete this annual induction within a month of it being issued and that the material itself is under constant review and amended in light of any changes to policy or where it is appropriate to refresh content.

FB-I provided the Team with a number of documents relating to staff training and confidentiality:

- Confidentiality, Respect and Ethics at Facebook
- Safety Training for Users Operation Team
- Complete confidentiality training
- FB-I employment agreement
- FB-I Potential Employee Non-disclosure Agreement
- Facebook Temporary Worker Orientation

The Office of the Data Protection Commissioner carried out a review of the documents which provide detailed information to staff on subjects such as how to deal with requests for user data, suicide and pornography reports, privacy settings, confidentiality of user data, Facebook's Privacy policy, system access controls and data security. Temporary staff receive security training as part of their work orientation which cover email and laptop security and security of confidential documents.

The Inspection Team discussed the content of the documentation with FB-I in detail. Where appropriate in the course of these discussions, the Team made recommendations as to content, which FB-I accepted. Prior to the completion of the audit, FB-I informed the Office that these recommendations have already been implemented and provided an updated copy of the relevant training documentation.

Chapter 3 – Subject Matter Areas Examined During the Audit

3. 1 Privacy Policy / Data Use Policy

3.1.1 Introduction

The ability of individuals to provide a meaningful consent to organisations for the use of their personal data is the subject of continuous debate and discussion. It was also recently addressed by the Article 29 Working Party in Opinion 15/2011 on the Definition of Consent[9]. This has outlined all the factors necessary to make consent valid. Of course it has also indicated that consent is not the only basis for the legitimisation of processing of personal data.

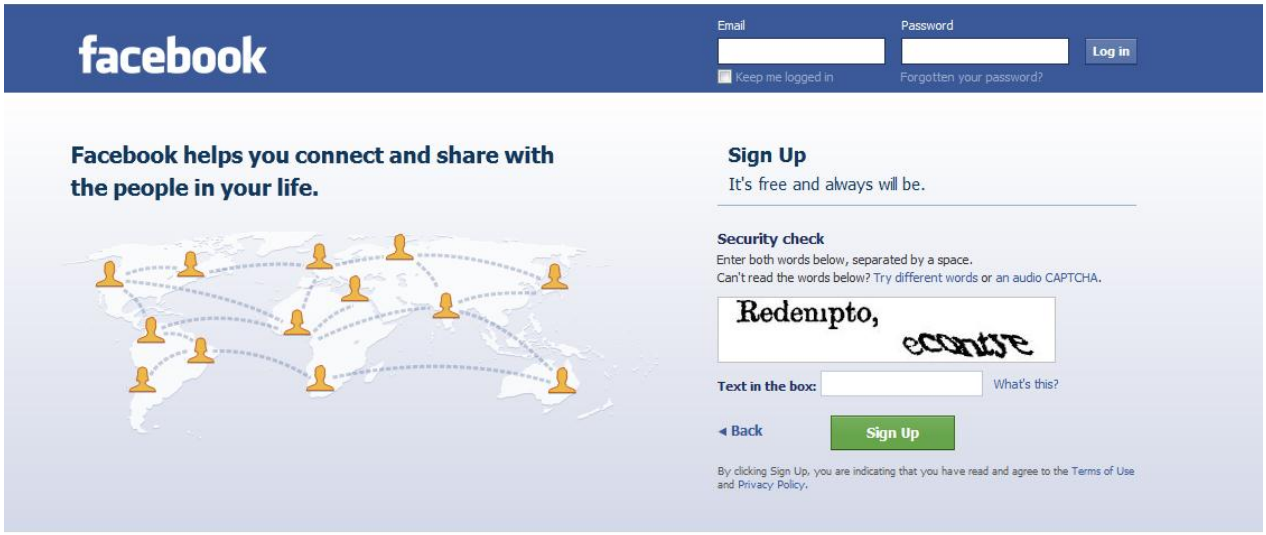
Obtaining - or assessing - meaningful consent is particularly challenging in the online environment. In the online environment, a user is often seeking to access a service as quickly as possible, and the presentation of lengthy privacy policies or terms and conditions which must be agreed to before proceeding may not create an effective means of capturing consent. This is even more difficult in situations where consent is collected via a tiny screen on a mobile device.

In the case of a social network, a user provides consent upon registering to the service. While the challenges outlined above are present, there is nevertheless an opportunity for a person to read the information provided prior to providing his or her personal data. Facebook, via its two page sign-up page outlined below, collects basic information and states to the user that by clicking sign up they are indicating they have read and agree to the Privacy Policy and the terms of use which is more commonly known as the Statement of Rights and Responsibilities.

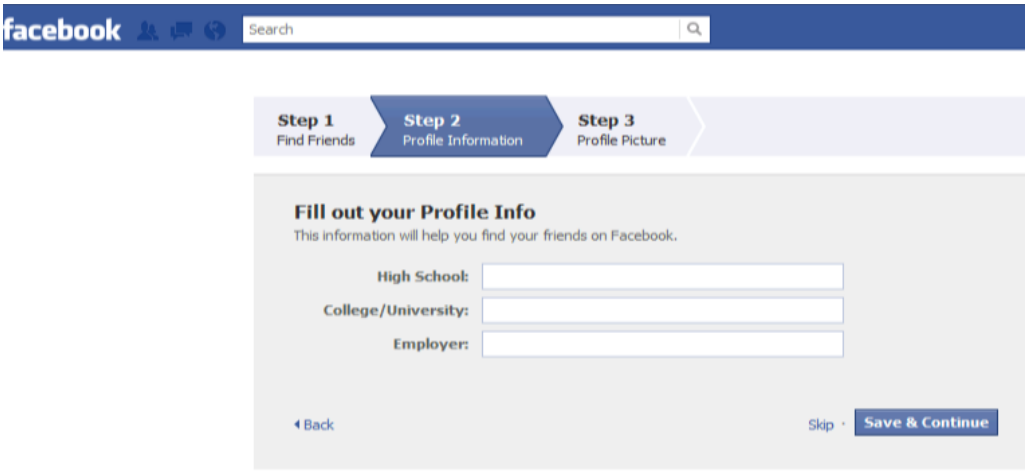
The issues around the capture of meaningful consent in this space are even further amplified when the consent is required from a minor. It can be assumed going forward that in more mature markets, at least, a large proportion of new users to Facebook will be minors joining a social network service for the first time. While Facebook does have additional protections for the data of minors which are outlined in Appendix 6 and an educational security centre for minors accessible at https://www.facebook.com/safety/groups/teens/, there is no distinction in the sign-up process as outlined below.

[9] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

3.1.2 Registering for an Account



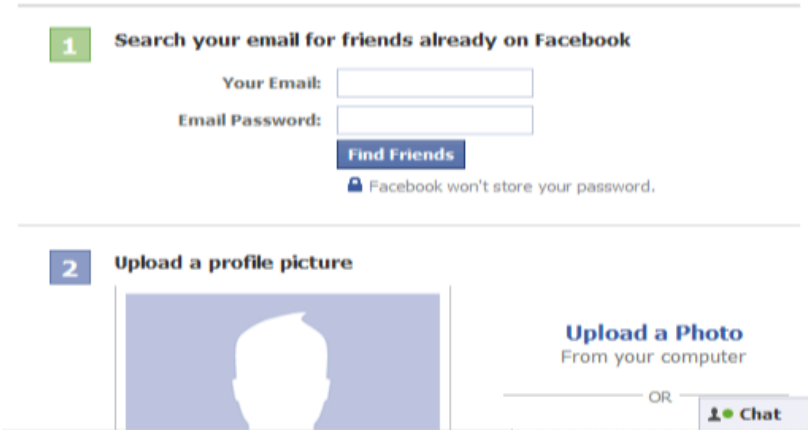
After registering, a new user is presented with a screen that encourages them to provide their contacts list to find friends on Facebook. This can be skipped. The new user is then presented with a screen (as below) to provide additional profile information. At present this could be termed as reasonably basic information and it is obviously of importance that this screen is not extended to seek additional information at this point before a new user has any opportunity to comprehend the use that will be made of such information. The screen can be skipped but it can be expected that most users when presented with fields of information to complete will do so.



Once this screen is complete a new user is encouraged to upload a profile picture. It can also be skipped if desired. It will be notable that no specific information is included on this screen as to the use of the profile picture.

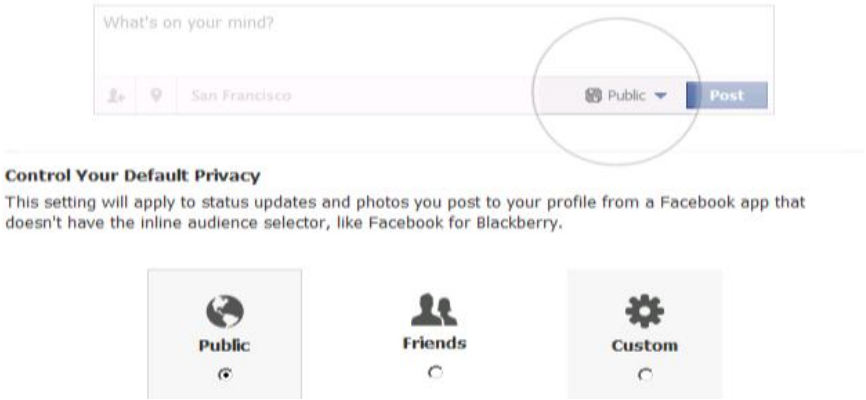
Thus by the above process a person becomes a Facebook member. Of course, at the point of sign-up a person could not reasonably be expected to fully understand or comprehend what it means in practice to have consented to the use of their data in this way.

It is notable that when the sign-up process is complete, the user is at no point encouraged to access their privacy settings and therefore the default settings apply. The default settings are outlined in the following screens. An issue which needs to be addressed in this area however is that there is a distinction to be drawn between the settings which are essentially about the user exercising control over how their information is presented and available to others that use Facebook and the settings which determine how Facebook can use that information. While the Data Use Policy addresses the use made of the data by friends and that made by apps for commercial purposes separately, the lines between both might not be easily understood by users.

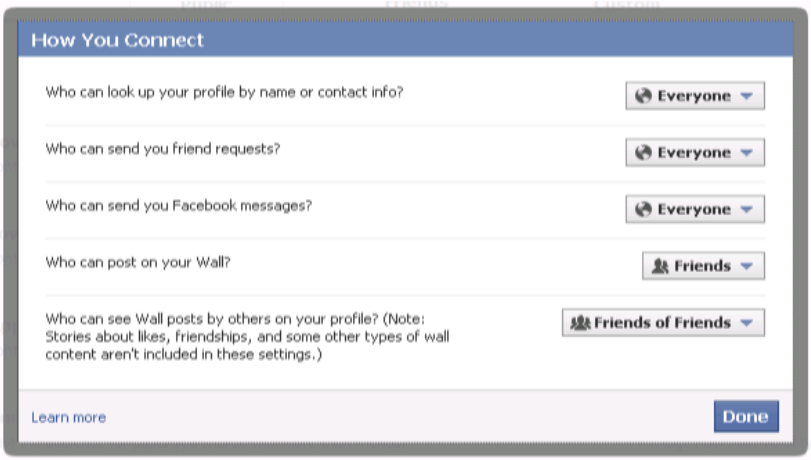


3.1.3 Settings

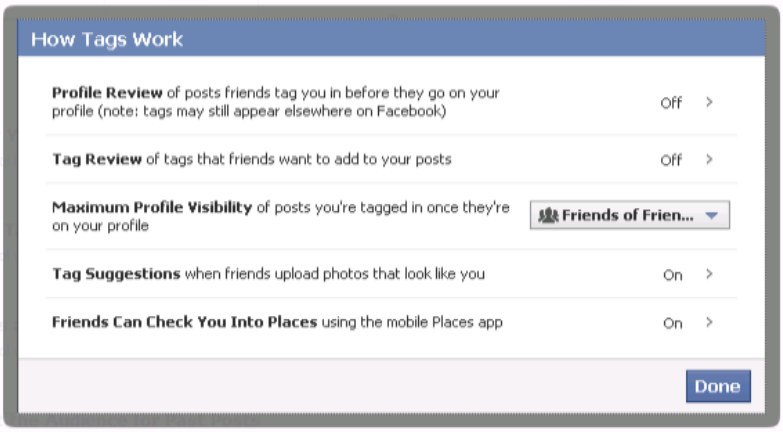
The default setting for status updates and posts which do not have an inline privacy control are public. FB-I has stated its view that the content that does not have an inline privacy setting is limited.



The default settings for connections are also at the maximum for availability with the exception of who can post on a user's wall, which is set at friends only.

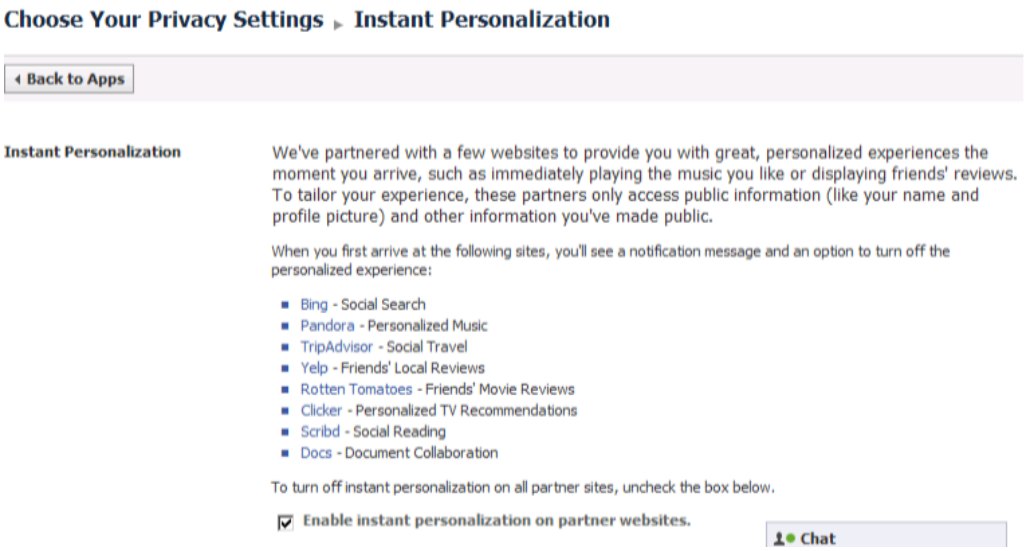


The default Tags review settings could be considered even more open and if maintained by a user, afford the user almost no control over such tags as they relate to them. FB-I's view is that users have control over their tags even if the default setting is not changed by being able to un-tag themselves and opt to pre-approve tags before they appear on their profiles.



Third Party Apps are dealt with separately in this Report. It is notable however that the default settings when apps are turned on is that a friend can allow an app that they sign up to access by default almost all relevant information about a user. In the Third Party Apps section we have outlined a concern about the accessibility and functionality of the tools available to users to prevent apps loaded by friends from accessing their information.

A feature introduced by Facebook some time ago is what is known as instant personalisation. This is a feature that provides what is termed basic user information to certain websites that Facebook has entered into a partnership with when a logged-in user visits such sites. The list of such sites is outlined below. Again it will be noted that the enabling of instant personalisation is turned on by default. *FB-I indicated, however, that this service has numerous data protection features built into it and that this feature is in limited use.*



The public search of basic profile information including photo if uploaded is also enabled by default.

It is therefore not surprising that the issue of consent as conveyed by the Privacy Policy and the Statement of Rights and Responsibilities were the subject of complaints received and which were therefore assessed in the audit.

3.1.5 Complaints Received

Norwegian Consumer Council

The complaint highlights a number of changes made by Facebook to privacy settings functionality. In one instance in December 2009, the Council considers that the new privacy settings recommended by Facebook would allow certain information, for example 'posts by me' and 'religious views' to be available to a wider user audience and that "members were urged to accept the new privacy settings". Facebook's 2009 privacy changes, including the way in which Facebook communicated the new settings to users, were a substantial focus of the recent FTC complaint and settlement with Facebook.

The Council also takes issue with another change, stating that, formerly, it was possible for a user to block all third party applications with a simple click, but now they had to be removed individually. FB-I noted that the single-click opt out was returned a year ago.

In **Complaint 8 – Consent and Privacy Policy**, Europe-v-Facebook contended that Facebook bases the processing of all personal data on the consent of the user to its Privacy Policy. The complaint set out two broad issues to be addressed in relation to the Privacy Policy, the first in relation to

the access to and content of the policy and the second in relation to consent. On accessibility the complainant contended that Facebook's Privacy Policy is not easily accessible – the link 'privacy' provided at the bottom of the user's Facebook page is merely a link to a privacy guide, containing limited information. There is a link within this document to the actual Privacy Policy.

FB-I did not share the complainants view in relation to the accessibility of the Data Use Policy since the Data Use Policy is accessible from virtually every page of Facebook, except for the user's profile page. Moreover, its visibility will be soon increased. A link will be added on the left-hand side of the newsfeed page for every user. FB-I also considered that it has gone to great lengths to ensure that it is available and easy to understand by users. The new Data Use Policy launched in September 2011 provides a clear view of the type of data collected, the privacy settings that users are encouraged to use to control their data, the information that is shared with other websites and applications, how the data is used in the context of the advertising services and also included a specific section about minors. The Data Use Policy is constantly amended to ensure that it captures FB-I's practices and provides users with the most accurate, precise and clear information.

Role of FB-I and the User: the complainant stated that the user is not provided with any clear information on who is the data controller (Facebook Ireland or Facebook Inc.) and that, if the identity of the data controller is unclear to the data subject, then the data subject cannot be considered to have provided his consent to the processing of his data.

FB-I stated that there is no confusion in relation to the identity of the data controller, stating that any non-US or Canadian user can see the following information:

> *The website under www.facebook.com and the services on these pages are being offered to you by: Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland*
>
> *However, FB-I is willing to provide clearer information to its users. Therefore, it has decided to add in the Data Use Policy the contact details of FB-I and a clarification about where FB-I is the data controller.*

Extent of Privacy Information: the complainant was dissatisfied that, in order to get a grasp of Facebook's privacy policies, a user must deal with multiple documents and links, with many specific provisions difficult to locate.

FB-I indicated that it updated its Data Use Policy in September 2011 to make it more user friendly.

Contradictions: the complainant highlighted contradictions he has identified within the Privacy Policy. He states that the contradictions identified run to 6 pages and has provided some sample issues in the complaint in relation to the deletion of data, for example, *"If you are uncomfortable with sharing your profile picture, you should delete it."* While elsewhere in the policy he points to the fact that *"Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere…"*

FB-I disagreed with the complainant that the Data Use Policy contains contradictions. In the above-noted example, in particular, FB-I discloses to users that information shared on Facebook

can be re-shared, and, in the second quoted part of the policy, stresses that one's profile photo may be shared so if the user feels uncomfortable with that, he or she should delete it.

Vague Provisions: the complainant highlighted a number of provisions in the Privacy Policy which he considers to be vague and general in nature, for example, *"We use the information we collect to try to provide a safe, efficient, and customized experience."*

FB-I disagreed that provisions in the Data Use Policy are vague and general. General statements in the Policy are followed by more specific statements, along with explanation and/or examples.

Unambiguous Consent: the complainant highlighted a number of issues with the process of consenting to the Privacy Policy including the use of small text and lack of a check box to be ticked.

FB-I provided a number of legal arguments in support of its view that Facebook is not required to provide a specific opt-in and stated that users, through their continued use of Facebook services, "continually manifest an unambiguous desire that their personal data be processed." That said, users are clearly informed in the Data Use Policy that Facebook may obtain personal information as a result of all interactions they have on Facebook. In addition, users are fully informed of the purposes of the data processing, including the customisation of the services offered and the protection of other users: "We may use the information we receive about you in connection with the services and features we provide to you [and] … as part of our efforts to keep Facebook safe and secure."

Freely Given Consent: this aspect of the complaint is in relation to the lead position Facebook has in the social networking business at present and that there should be a high bar in terms of privacy terms and conditions given Facebook's position in the marketplace.

Specific Consent: the complainant contended that there is no specific consent being provided by users for the use of their personal data.

FB-I disagreed with the complainant's assertion and pointed to the fact that specific consent is provided by the user agreeing to the Data Use Policy and through the user's on-going use of Facebook, including the opportunity to review and comment upon any revisions to the Policy (and possibly vote on them) prior to the Policy going into effect.

Informed Consent: the complainant considered that the purpose for which personal data is being processed is not being properly explained.

FB-I did not share the complainant's view that the processing of personal data is not being clearly explained. The Data Use Policy describes the type of data collected, the privacy settings that users are encouraged to use to control their data, the information that is shared with other websites and applications and how the data is used in the context of the advertising service. The information is provided in a clear and understandable format. That said, Facebook is always willing to improve the format of its Data Use Policy to lead the efforts of the industry with regard to privacy education.

Consent obtained by deception or misinterpretation: this related to how Facebook used personal data and the complainant highlighted a number of examples where he considered Facebook to be providing false or misleading information, for example, the fact that users are told they can remove posts, pokes, etc, but that they are not, in fact, being deleted but being held in the background. He also complains that some functions, such as deleting your account, are hidden from view. These aspects of the complaint are dealt with separately in the Report. *FB-I categorically denied that it engaged in any deception, although recognized that "remove" could have been interpreted by users to mean that the data was deleted.*

The issue of consent is also addressed in **Complaint 16 – Opt Out** from "Europe-v-Facebook". This complaint covers a number of areas relating to the set up of a new Facebook account. The first issue raised by the complainant is that there is no specific consent when signing up to Facebook. The complainant argued that Facebook collects a range of data (import of email addresses, education information, photograph, etc.) from the new user before that user is provided with an opportunity to change his security settings and that a link to privacy information is only provided once the sign up process is complete (the link is available on the second page as demonstrated above).

FB-I in response to a query from this Office indicated that the account is not set up until the potential user has successfully transmitted a Captcha phrase (this is a code sought on many websites to counter malicious automated computer processes from gaining access to services),which is not done until the potential user has seen the links to the Data Use Policy and the Statement of Rights and Responsibilities. FB-I also indicated that if an individual does not complete the registration process, the registration form data is deleted.

The complainant also contended that the default security settings themselves are too liberal in nature in that the initial user content may be seen by most people and can be indexed by search engines. Finally, the complainant considered that the settings pages and links provided discourage the new user from applying certain security settings and points out that some important settings cannot be edited on a user's main page, for example, access by third party applications and search engines.

FB-I contended that it does receive the specific consent of Facebook users. In relation to the collection of data when signing up for an account, Facebook stated that it is not possible for a user to adjust their security settings prior to the account being created, but highlighted that once it is created, the user can make whatever amendments he wishes. FB-I also highlighted that only name, email and date of birth are required to create an account – any other information is optional.

FB-I stated that the complainant's contention that users are deliberately discouraged from applying certain security settings and that some settings are 'hidden' to be unfounded. The security centre and Data Use Policy encourages users to practice judgment when sharing content and data on the site. FB-I considered that the content of its privacy settings are presented in logical order and that detailed explanations of the settings are also provided.

Complaint 18 – Obligations as Processor from "Europe-v-Facebook" contended that Facebook's operation as a processor is at variance with both Irish Data Protection legislation and Directive 95/46/EC. The complainant states that Facebook and its users can only process data legally if

Facebook clearly defines, in relation to each piece of data held, who is the data controller and who is the data processor. This issue is dealt with in the introduction to this Report by reference to what is termed the household or domestic exemption and the responsibilities of a business for instance when using the site.

Complaint 22 – New Policy from "Europe-v-Facebook" related to what are stated as recent changes made to Facebook's Privacy Policy. The complainant contends that it is difficult to understand the changes in conjunction with the previous policy and that users have not had any opportunity to consent to the changes made. In light of the recent comprehensive FTC settlement with Facebook in thus area, the question of consent in relation to the new Privacy Policy will not be considered in this report.

3.1.6 Analysis

This Report has demonstrated that Facebook by its very nature is a complex and multifaceted online experience that has enjoyed remarkable success by virtue of the number of members and active users in a very short period. It is seen as an essential part of the routine of at least 800 million users who log on every month. Any assessment of the privacy policy and consent must have due regard to these realities. However, the role of this Office is to assess matters from a purely data protection perspective.

In the assessment of this Office the operation of the privacy controls available to users within Facebook are complex. This is despite efforts by Facebook to simplify the settings in order to make them more easily understandable and usable. As our analysis in this Section and other sections demonstrate there are a multitude of different controls that must be accessed by the user to express their preference in relation to the use of their personal data. In addition to the controls available from the privacy settings, there are separate and distinct controls for Apps, for Ads and for Security. In order to fully understand the use of their information and the options available to them a user must read the full Privacy Policy, the Statement of Rights and Responsibilities, the advertising policy, information on the use of social plugins, information on Facebook Credits etc. It is clearly impractical to expect the average user, never mind, a thirteen year old joining the site for the first time to digest and understand this information and make informed choices. The difficulty in this area is further exacerbated by the fact that the choices which a person should make when joining or thereafter once they have begun to understand the social nature of Facebook are not in any real way presented to them in a manner in which they can fully understand and exercise real choice.

The problem of effective choice and control of a user is made more problematic by the default settings which Facebook has chosen for the user. Many of the default settings for adults (though not for minors) are set at what might be considered the most liberal possible. Facebook in this respect is obviously entitled to assert that social networking by its very nature is social and there is no point joining that experience if the person does not wish to interact with others. This is accepted but the combination of liberal default settings and the lack of a uniform method to present privacy choices to users is not reflecting the appropriate balance in this space. *FB-I indicated that it believes it has made great improvements in providing users better control over their privacy settings by moving most of the settings inline. This means that users with every new post or comment or upload can see the audience with whom they are sharing at the precise*

moment that information is most relevant and choose precisely the audience they want rather than having to refer back to a setting page.

A specific example outlined above related to the upload of a profile photo when joining. At no point in that process is it clarified to the user that by uploading their photo it will be by default publicly searchable until they change the setting and that furthermore their profile photo once uploaded will be used in a range of scenarios including advertising purposes to their friends with varying levels of control. FB-I could legitimately say in response that it would be abundantly clear to a user from using the site that their profile photo would be used in this way but it clearly would not be in any way clear to a new user.

Another issue which was legitimately highlighted in the complaints from "Europe-v-Facebook" was that 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 were much smaller than the remaining information on the page. We have accordingly recommended to FB-I that this matter be addressed and it has agreed to do so.

However, the concern of this Office is not focused on specific issues such as these but rather the bigger picture around appropriately informing, in a meaningful way, a new or current user and then providing easy to use and accessible tools to users. In this respect it is notable that if a user or new user does not add a certain number of friends or provided certain details in the sign-up process that they are constantly reminded to do so on their profile page or upon log-in. There are no such reminders or prompts about the desirability of selecting privacy settings that the user is comfortable with or adjusting them over time in light of their experience or where they are in their lives at a particular time.

From the privacy perspective therefore it would be a far better position for users if there were no default settings upon sign-up. A user then would be asked via a process what their broad preferences are with settings that reflect such broad preferences and a consequent ability for the user to refine those settings all of which should be available from one place. This Office has no difficulty with FB-I expressing its position as to what it believes a person should select to gain the greatest experience from the site but we do not accept that the current approach is reflecting the appropriate balance for Facebook users. By extension it is clearly the case that the process also needs to be adjusted for current users to take account of this approach. This Office therefore recommends that FB-I undertake a thorough re-evaluation of the process by which it empowers its users both new and current to make meaningful choices about how they control the use of their personal information. This Office does not wish to be prescriptive at this point as to the eventual route chosen but expects FB-I to take full account of the suggestions outlined above. This is clearly an issue which will form part of an ongoing engagement with FB-I and which will be thoroughly reviewed in July 2012.

Although FB-I indicated that not only has it endeavoured to make its Data Use Policy as simple to read and understand as possible, and offers a notice, comment, and voting period on material changes to its policies, it is committed to reaching an agreement with this Office on a solution that will satisfy the concerns expressed in relation to enhancing user awareness and control over their privacy settings. The agreed shared objective in this respect is to ensure that users are provided

with ample opportunity to express, in a fully informed manner, their choices as to how their information is used and shared on the site.

However, again it is important to draw a distinction between the controls available to users to decide to whom (only me, friends, friends of friends, public etc) and how their information is available when they take certain actions on the site and the use made of data by Facebook. As we stated at the outset of this Report, we do not believe that data protection law can be interpreted to place an obligation on Facebook to provide a free service to users without some base line serving of ads based on user information. To a point the extent of FB-I use of basic user data for ad targeting purposes could arguably be legitimised by either consent or legitimate interests. The question that arises in this regard is exactly how much information is enough for Facebook in this area. As outlined in the section on advertising Facebook's policy is that it does not allow the serving of ads based on the use of sensitive data as defined under EU law. In practice, however, it does seem that it is possible to use such information as contained in a profile. In this respect, it is not inappropriate for FB-I to claim legitimate interests for the processing of profile, interest and 'like' information entered by a user if it were considered that consent would not be a sufficiently robust basis for such processing. Regardless, there needs to be full information on such use and as outlined in the Advertising Section we consider that additional information is required.

This Office is aware from our audit that Facebook already carries out user testing using a third party company to test how users and non-users react to new products etc. We would recommend, therefore, that a valuable insight could be gained by FB-I by testing any approach to be developed with both users and non-users. FB-I agrees that it will continue to do such testing and will take account of the outcome of this audit in this regard.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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	FB-I will work with the Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate.	End Q1 2012 and routinely thereafter
	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.	Agreed. Furthermore, FB-I has agreed to take the additional step of moving the links to the Data Use Policy and other policy documents, as well as the Help Center, to the left side of the user's homepage. Presently the use of Credits is required only for games that monetise through virtual goods.	End February 2012

3.2 Advertising

It is not a secret that the means of funding the operation of Facebook as a free platform for members to engage in social networking is via various forms of advertising from third parties to those members. What is perhaps less clear is what precise user information is used by Facebook to make its advertising proposition attractive to advertisers. Therefore in this audit we sought to clarify this position and where appropriate seek enhanced information and control for members as to certain information which can and cannot be used for targeted advertising purposes.

As stated in the previous section on the Privacy Policy, it is important to make clear at the outset that 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.

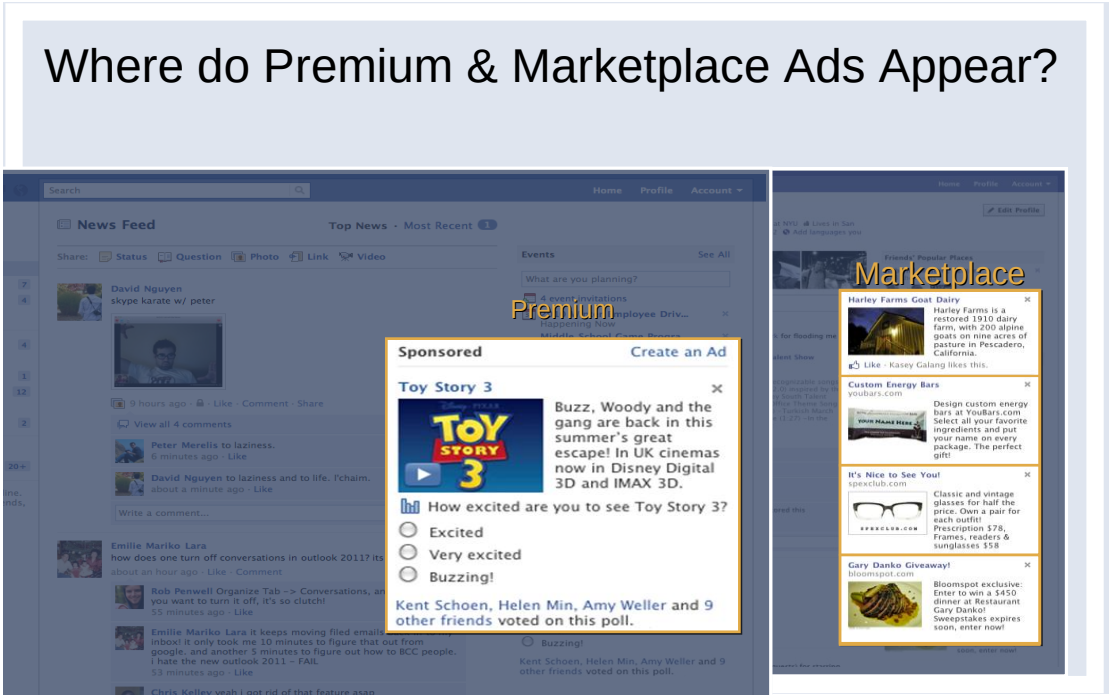
3.2.1. Advertising Operations

Advertising Operations is a division of FB-I with a staff of 33. The Advertising Operations Division manages advertising campaigns on behalf of FB-I. To assess the level of use of Facebook members' data for advertising purposes the Office met with relevant team members.

FB-I offers two basic advertising models to its advertising customers: **Premium Ads and Marketplace Ads.**

Premium Ads are ads which appear uniquely on a member's profile/timeline or newsfeed utilising 100% of the homepage space available for advertising (see screenshot below). FB-I confirmed that only a limited number of "managed clients" are able to purchase premium ads. Such managed clients are handled directly by the Inside Sales team based in Dublin or the Direct Sales team based in the European local offices. An advertiser cannot purchase a premium ad using the online tools available on Facebook and are set up by the Facebook advertising operation team only.

Marketplace Ads are ads which appear to the right hand side of all Facebook pages, except for profile pages. Up to 6 of these ads may appear on a page (see screenshot below). All clients may purchase marketplace ads. Pricing for such ads are set via automatic auction. Potential advertisers bid either for the price they are willing to pay every time their ad is clicked (pay-per-click model) or they bid what they will pay every time a set number of impressions are displayed (1,000 impressions model).



If a user clicks on an ad in Facebook they are either taken through to the page created by the advertiser on Facebook itself or alternatively, the user may be taken to an external website.

Users will generally encounter three basic types of advertising on Facebook:

a) Personalised Adverts
b) Adverts + social context
c) Sponsored Stories

Details of such advertising is provided in the "How Advertising Works" section of the Data Use Policy[10].

Featured Content consists of Facebook's promotion of its own features and fell outside of the scope of this audit.

(a) Personalised Adverts

In its Data Use Policy Facebook provides the following description of its personalised advertising:

> *When an advertiser creates an ad on Facebook, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users. For example, an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball.*

The Data Use Policy goes on to note:

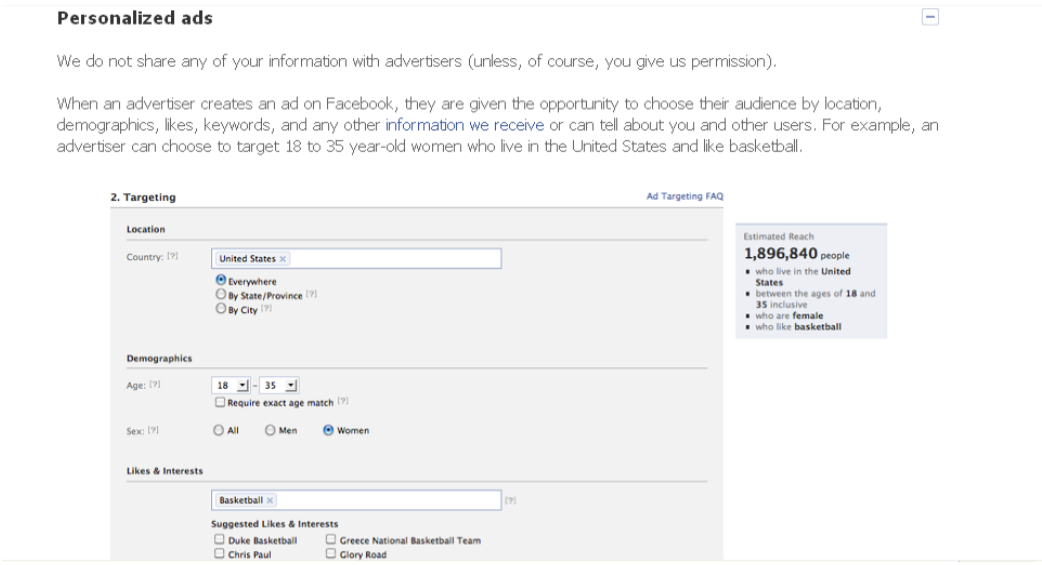
[10] http://www.facebook.com/about/privacy/advertising

Sometimes we allow advertisers to target a category of user, like a "moviegoer" or a "sci-fi fan." We do this by bundling characteristics that we believe are related to the category. For example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theatre, we may conclude that this person is likely to be a sci-fi fan.

A significant focus was placed on examining the bundling characteristics process for advertising targeting purposes. The disclosure above does not mention the use of user messages or chat to target ads, and FB-I confirmed *that the content featured in user messages or chat was not used for that purpose. Rather, ad targeting is based on actions as described in the above disclosure, such as the pages on Facebook that a user has "liked." Where Facebook allows content featured in status updates or posts to walls to be machine read to target ads based on that content, these keywords obtained in that manner are not retained.* FB-I has undertaken to revert to this Office in the event that it proposes to extend the items of data to be considered for more granular targeting of the user.

During the course of the discussions on advertising, FB-I provided information on a trial use of certain limited keywords within wall posts and status updates for ad-targeting purposes. For example, FB-I stated that if a user mentioned a car in a status update and also "liked" something related to cars, FB-I might target ads to the user at a potential car buyer. As it was apparent to FB-I from initial consideration that this use caused some unease on the part of this Office, it offered to suspend the "trial" of this service until such time as the matter could be discussed in more detail following the conclusion of the audit process. This was agreed and this issue will be revisited in January.

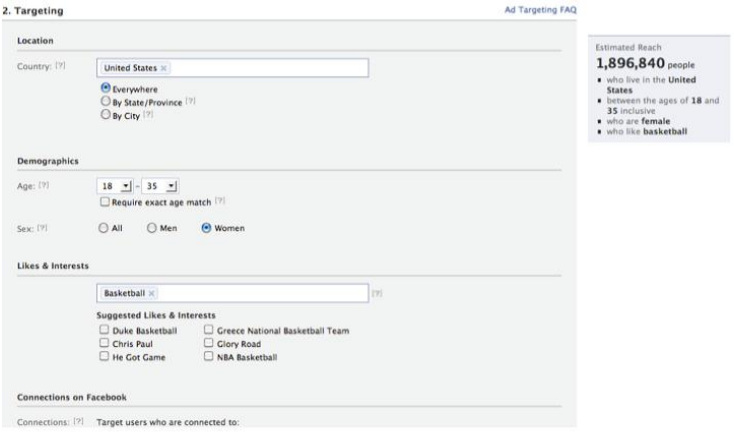
The Data Use Policy contains a screenshot visually demonstrating part of the ad creation process.[11]



It also invites the Facebook users to

"Try this tool yourself to see one of the ways advertisers target ads and what information they see at: https://www.facebook.com/ads/create/ ."

[11] https://www.facebook.com/about/privacy/advertising#personalizedads

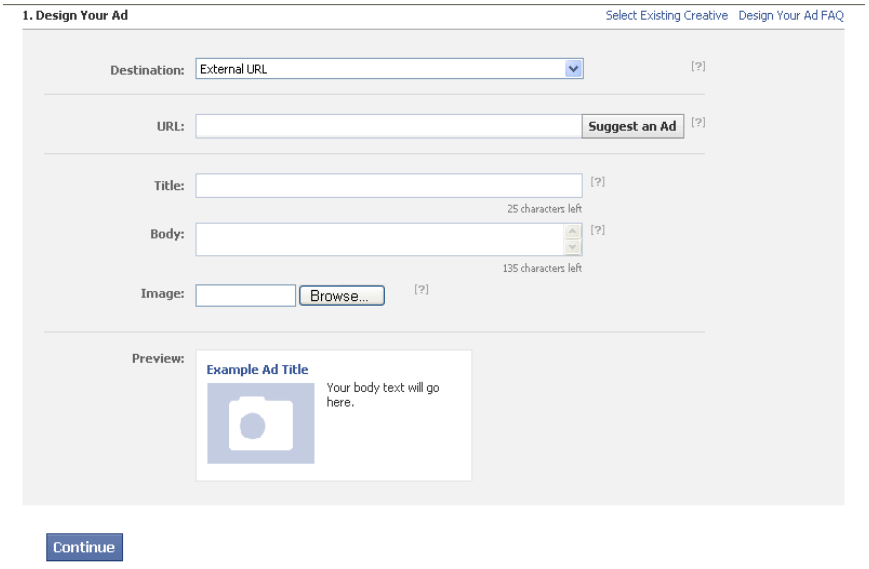


Try this tool yourself to see one of the ways advertisers target ads and what information they see.

If the advertiser chooses to run the ad (also known as placing the order), we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are. So, for example, if a person clicks on the ad, the advertiser might infer that the person is an 18–to–35–year–old woman who lives in the US and likes basketball. But we would not tell the advertiser who that person is.

After the ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads.

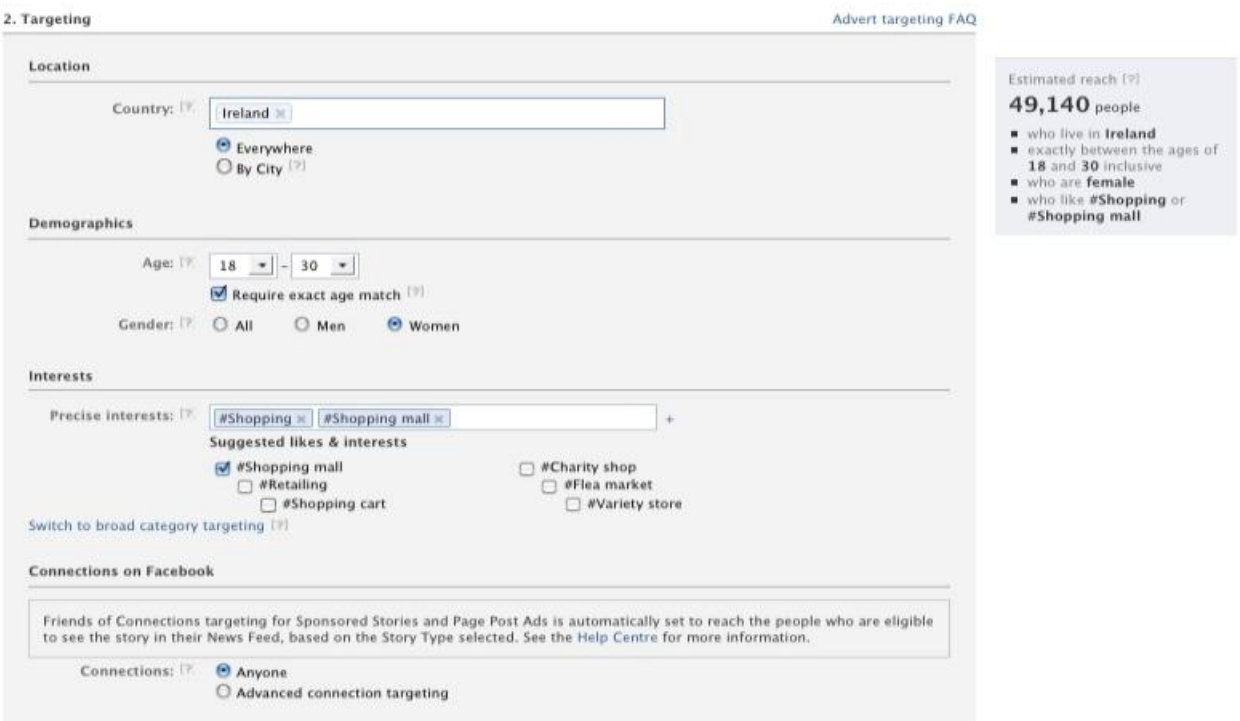
This link brings the user the Ad Creation tool:

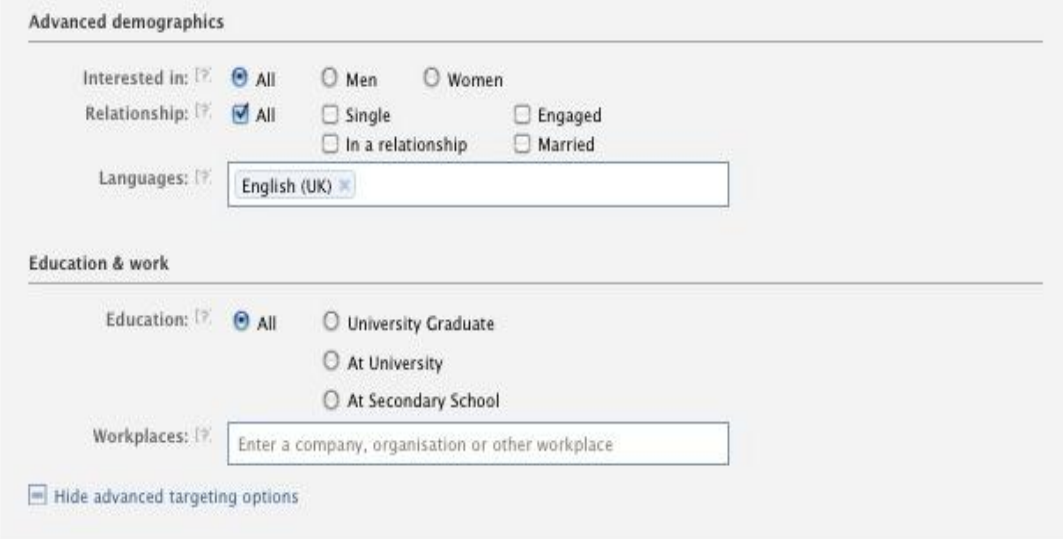


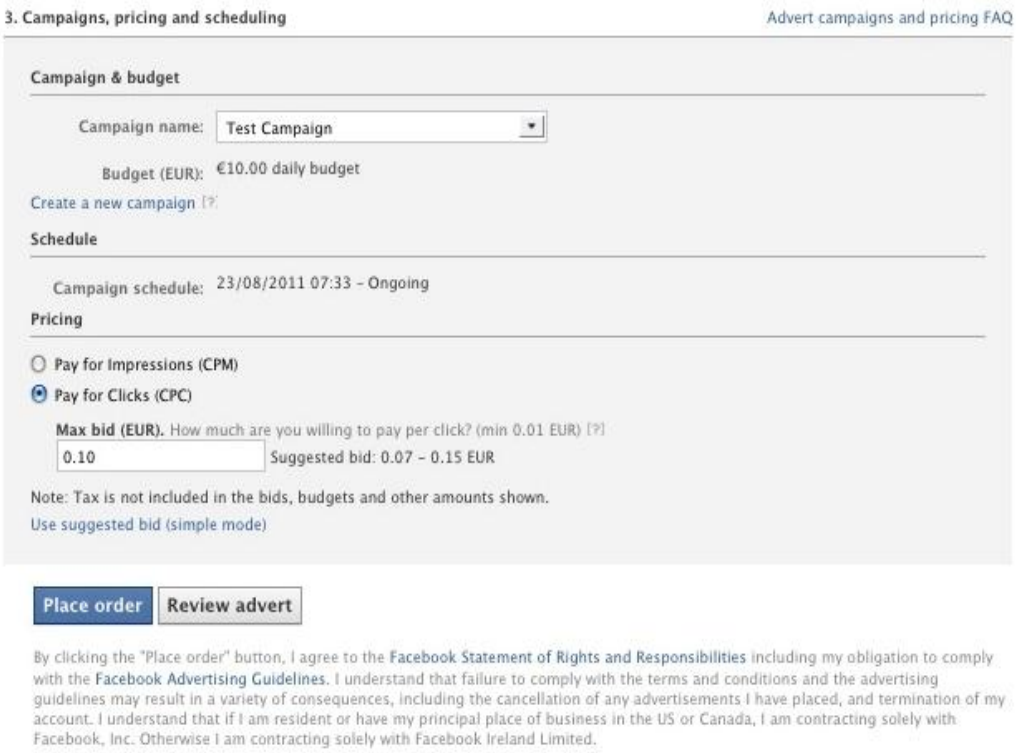
Here, users can try out the tool and create their own ads, thereby seeing how advertisers can target ads.

FB-I has indicated that the following screens represent the full screens on which an advertiser purchasing advertising through Facebook's online tool would create an ad and enter their preferences for targeting purposes:


Advertise on Facebook
Account: #56821200 (Erica Test Account, EUR)
1. Design your advert
Select Existing Creative
Design your advert FAQ
Destination
External URL
URL
www.example.com
Suggest an advert
Title
Example title
12 characters left.
Body
Example ad text
120 characters left.
Image
Browse...
Remove uploaded image.
Preview
Example title
Example ad text


2. Targeting
Advert targeting FAQ
Location
Country:
Ireland
Everywhere
By City
Demographics
Age:
18
30
Require exact age match
Gender:
All
Men
Women
Interests
Precise interests:
#Shopping
#Shopping mall
Suggested likes & interests
#Shopping mall
#Retailing
#Shopping cart
#Charity shop
#Flea market
#Variety store
Switch to broad category targeting
Connections on Facebook
Friends of Connections targeting for Sponsored Stories and Page Post Ads is automatically set to reach the people who are eligible to see the story in their News Feed, based on the Story Type selected. See the Help Centre for more information.
Connections:
Anyone
Advanced connection targeting
Estimated reach
49,140 people
who live in Ireland
exactly between the ages of 18 and 30 inclusive
who are female
who like #Shopping or #Shopping mall





As outlined above it is important that Facebook is transparent with users as to how it uses information provided by users to target advertisements. In terms of the other categories listed in the 'Advertising Guidelines' which may not be used to target ads to individuals such as 'religion or philosophical beliefs' we are aware that when an individual is creating or editing their profile the following screen will appear under the tab 'philosophy'.

We noted that the 'philosophy' area of a Facebook member's profile (see screen above) contains an area where a user can enter their religious or political beliefs.

The definition of sensitive data in Irish data protection law is:

> 'sensitive personal data' means personal data as to—
>
> (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
>
> (b) whether the data subject is a member of a trade union,
>
> (c) the physical or mental health or condition or sexual life of the data subject,
>
> (d) the commission or alleged commission of any offence by the data subject, or
>
> (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

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. 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.

(b) 'Ads' with Social Context

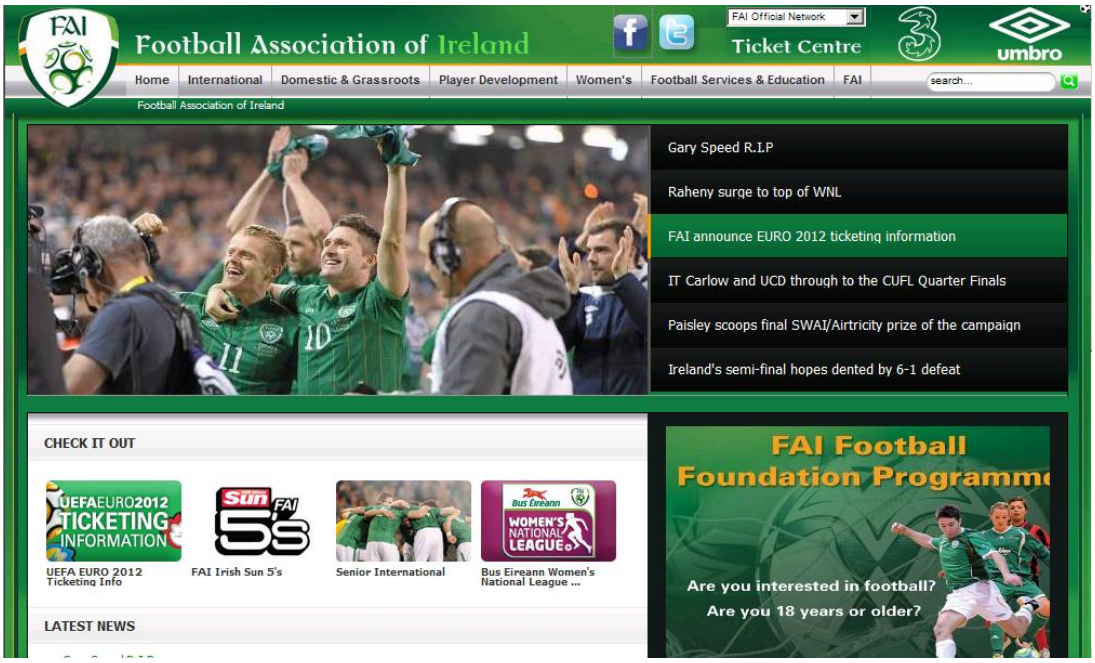
'Ads' with Social Context is an approach where the actions of users regarding different products or advertisements are linked to the user in ads to their friends on Facebook.

The Data Use Policy describes such 'Ads' in the following terms:

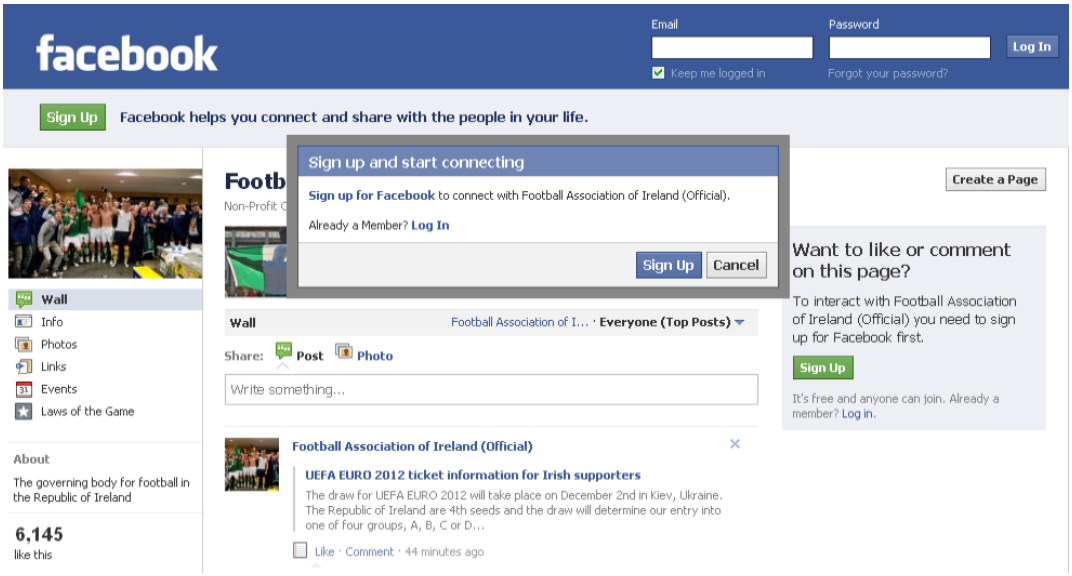
> *Facebook Ads are sometimes paired with social actions your friends have taken. For example an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page*.

As an example, if Jane, a Facebook member clicks ‘like’ on a sushi restaurant website, Jane and her friends will see in their newsfeed “Jane likes sushi city,” and her friends then may also be served an ad for “sushi city” on the right of their newsfeed showing that Jane liked it.

If a user is not logged into Facebook but instead comes across a product or an organisation’s website outside of Facebook and the website has a Facebook social plug-in on it, the user can click on this and be taken through to the product’s Facebook page where they have the opportunity to click on the “like” button. Once the user clicks on “like” they will be asked to sign up to Facebook or log in if they are a member. The following two screens demonstrate this scenario, with the first screen containing the Facebook ‘f’ button on the home page of the Football Association of Ireland.



Clicking on the ‘f’ button (top centre of screen above) takes the user to the next screen below.



3.2.3 Information collected from sites with Social Plug-ins

An issue which arose for substantial public comment in the immediate period before the audit was information which Facebook was allegedly receiving either intentionally or unintentionally in relation to individuals who visited the some 2 million websites that contain Facebook Like plug-ins. The process outlined in the section above relates to the use of information when a user actively "likes" something. Facebook also currently receives data when a user or non-user visits a website with a social plug-in. How much data it receives depends on whether the person has ever visited Facebook.com. There is a detailed analysis of Cookie usage elsewhere in this report and the technical considerations are at Section 6 of the Technical Analysis Report at Appendix 1.

As outlined in the Technical Analysis Report, this Office is satisfied that while certain data which could be used to build what we have seen termed as a "shadow profile" of a non-user was received by Facebook, we did not find that any actual use of this nature was made of such data and as outlined elsewhere in this report, FB-I is now taking active steps to delete any such information very quickly after it is received, subject to legal hold requirements The receipt of such data is in most cases attributable to the way the internet works with different content on websites delivered by different content providers. A Facebook social plugin embedded in a website is delivered by Facebook directly to the user's computer when a user visits that website with the means of delivery the IP address of the user's machine.

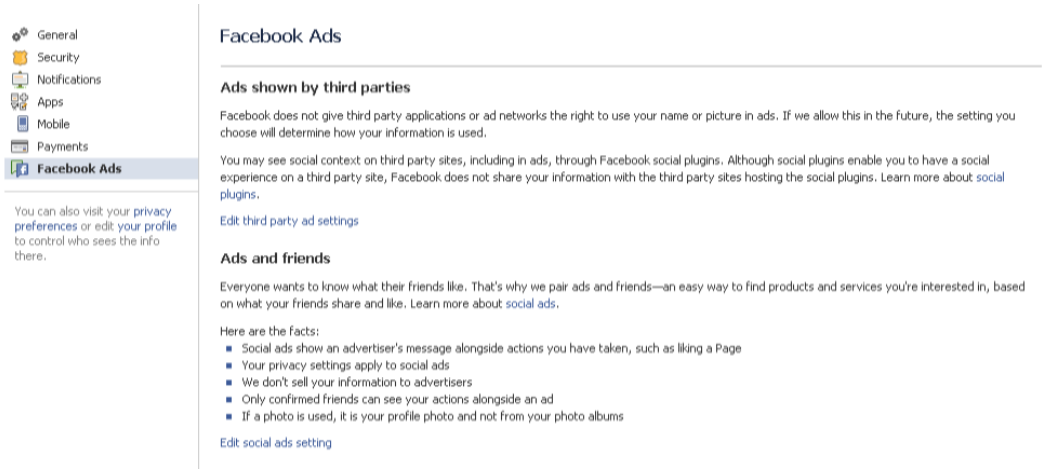
For the purposes of this section on advertising, FB-I has satisfied this Office that no advertising-related queries are served to the impression data collected from social plug-ins on websites either by way of IP address or Datr cookie information. However, as might be anticipated, if a logged-in user clicks on a "like" button, a connection is made that becomes part of the user's profile/Timeline and, in that regard, becomes part of the data that can be used to target ads.

We have separately satisfied ourselves by way of testing that browsing activity to sites with social plug-ins regardless of whether the user is logged-in or out does not cause any change in the ads served to users.

In terms of user choice the "**Data Use Policy" - IV How Advertising works** under **ads+ social context** states

> *If you do not want to appear in stories paired with Facebook Ads, you can opt out using our edit social ads setting*

Clicking through the link edit social ads brings the user to the following screen

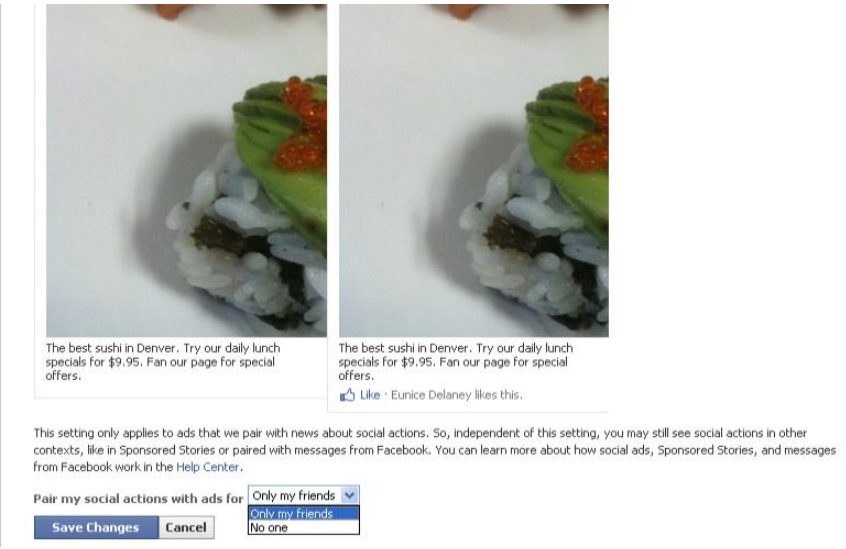


In terms of the location of the 'edit social ads' facility, we encountered difficulty locating the 'edit social ads' facility from the user homepage. It is available under "account settings".

['Account settings' is a menu item offered alongside 'privacy settings' in the dropdown list viewable to users who right click over the 'Home' Menu Tab in top right-hand corner.]

We recommend that the ability for users to exercise control over this feature is integrated into a user's privacy settings as opposed to being part of account settings. We have dealt with the ease of use of the privacy settings separately. FB-I has agreed to move these settings in line with its other privacy settings.

Clicking 'edit social ads' displays an option to *'pair my social actions with ads for...'* and a dropdown list set by default at '*only my friends'*. We verified that *'only my friends'* could be changed to *'no one'* as per the following screen.



However, editing social ads and resetting to *'no-one'* only prevented a user's social action, e.g., liking a product, from being paired with an ad for that product created by the advertiser. A user may still appear in a 'sponsored story,' which is a "story" that states the action the user took but is associated with the brand image rather than an ad created by the advertiser.

(c) Sponsored Stories

The Data Use Policy provides:

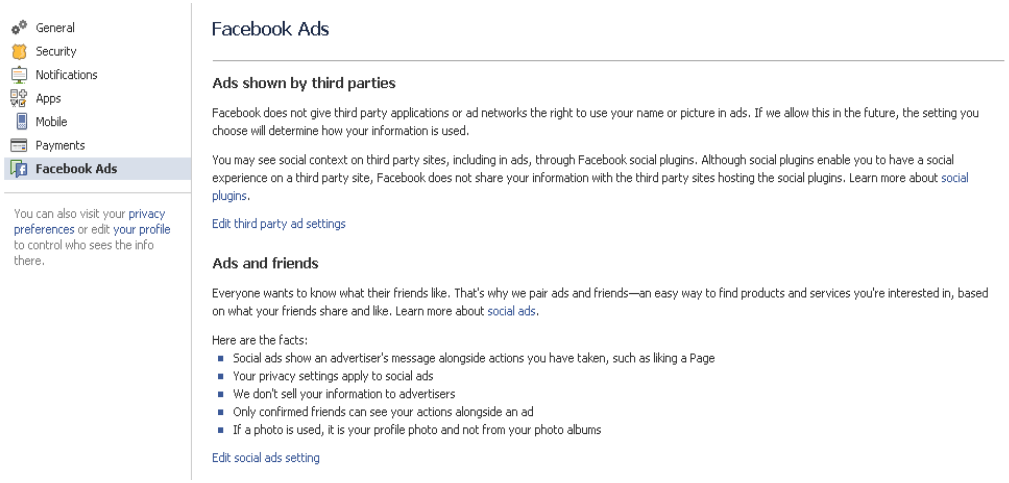
> *Many of the things you do on Facebook (like "liking" a Page) are posted to your Wall and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too. If they do sponsor a story, that story will appear in the same place adverts usually do under the heading "Sponsored Stories" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.*

This kind of story may appear in the marketplace ads section of the site or may appear in the news stream of the user's friends. Such sponsored stories utilise the user's image and therefore this Office is concerned at such use of an image photo without an ability for the user to exercise a choice. It is accepted that a user's profile photo (if they have one) is already available to their friends and that Facebook obtains consent for this use in section 10 of its Statement of Rights and Responsibilities, but this further use is not satisfactorily explained in the Data Use Policy. This Office therefore recommends that appropriate language be added to the Data Use Policy, which FB-I has agreed to do.

3.2.4 Ads displayed by third parties within applications

It is only possible for third parties to serve ads directly to users within applications on Facebook (see screen below). Developers cannot offer, however, social ads or sponsored stories within their applications. These ads are only served by Facebook.

It is noted that as per the 'edit social ads' settings the default setting is '*only my friends*' with the alternative setting *'no one'.*



Upon changing the default to *'no one'* confirmation of the change was signalled.

3.2.5 Ad targeting below 20 users

The Office 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. We are satisfied, following the audit that FB-I has put adequate safeguards in place to prevent this from occurring.

Until recently Facebook prevented advertisers from creating ads and sponsored stories with an estimated reach of less than 20 users. However, since the audit commenced Facebook has modified the way this system operates and advertisers targeting smaller audiences are no longer prevented from creating an ad when the audience estimate is less than 20. However, the ad is only delivered when the audience reaches more than 20.

3.2.6 Information Available to Advertisers

A frequent issue that arises in public comment is the level of user information that is made available to advertisers.

FB-I clearly stated that it does not share user information with advertisers without user permission. Facebook's Data Use Policy provides:

> *We do not share any of your information with advertisers (unless, of course, you give us permission).*

Facebook's Advertising Guidelines[12] state under **Data and Privacy**

> *Ad creative may not contain user data received or derived from*

[12] http://www.facebook.com/ad_guidelines.php

Facebook, even if a user consents to such use.

User data received or derived from Facebook, including information collected from an ad or derived from targeting criteria, may not be used off of Facebook without users' prior express consent (and only to User data received or derived from Facebook, including information collected from an ad or derived from targeting criteria, may not be used off of Facebook without users' prior express consent (and only to the extent such use isn't otherwise prohibited under applicable policies).

Any permissible data collection or use of user data must be consistent with Facebook's privacy policy and the privacy policy of the landing page and advertised site.

From a review of the advertising practices described above, this Office is satisfied that Facebook does not provide user data in breach of its Data Use Policy.

This Office has a concern, however, about the possibility of passive transmission of data such as an IP address when an advertiser has deployed a click tag (web beacon) and to meet these concerns recommends increased transparency, as well as monitoring and enforcement of its policy regarding click tags, which FB-I has agreed to do. This matter is outlined in further detail below.

We do note, however, that Facebook appears to reserve the right to, in the future, allow advertisers to make use of a user's publicly available information.

The Ads Shown by third parties section of the Account Settings provide that:

Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used

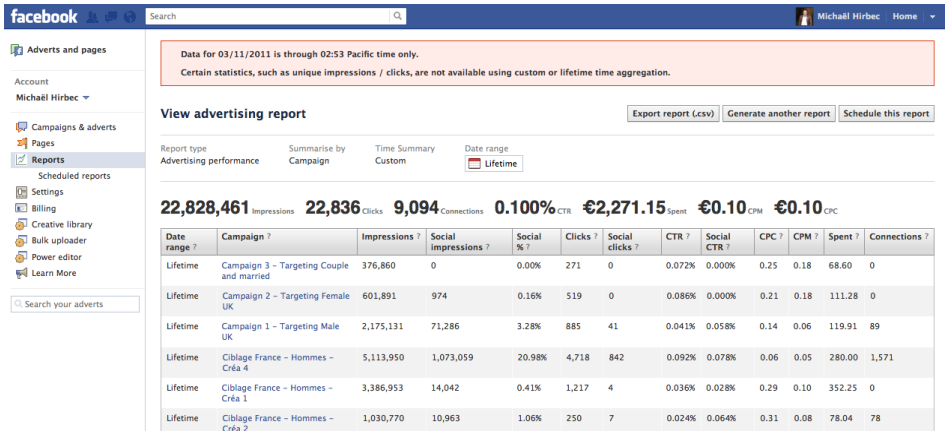
This Office considers that if, in the future, individuals' profile pictures and names are to be provided to third parties for advertising purposes, users would have to provide their consent. FB-I in line with its standard approach has indicated that it will enter into discussions with this Office in advance of any plans to introduce such functionality.

As noted above, we are satisfied that FB-I has established an advertising model which allows for targeting advertising without the provision of user data by it. This Office was aware, however, of the possibility that user data could still, nonetheless, be shared with advertisers, as part of, for example, dispute resolution processes.

To investigate this possibility we met with and interviewed the various teams who manage and promote advertising within FB-I. We also examined the various tools and systems available to staff members. We sought a detailed description and list of the various systems available to staff members throughout Europe and sought and received copies of the contractual provisions in place between FB-I and each of the Facebook entities established in Europe to manage access to any such personal data arising.

We commenced our analysis by examining the means by which FB-I interacts with advertisers. We noted that while FB-I does provide its advertising customers with detailed information about the effectiveness of their campaigns, it does so in an aggregated and anonymised format. As an example, one ad campaign examined was targeted at all users aged 13-34 in 8 major countries. Detailed information is available to the advertiser in relation to the number of times the ad was served, the click through rate etc per country. On a country level, information is broken down into region. So, for instance, information is available in France for Alsace, Aquitaine, Auvergne etc. but not at any lower level of detail. Information is also provided on the number of persons aged 13-17, 18-24 and 25-34 that accessed the ad and the breakdown between males and females. It is not possible to identify any individual from this level of detail. A sample ad campaign report is contained below.

Ad campaign report



Dispute Resolution

It is clear that occasionally a difference of opinion will emerge between an advertiser and FB-I as to the number of impressions of an ad or the number of actual clicks that took place. In this respect we wished to confirm that IP address information is not provided to advertisers in such circumstances. This was confirmed by FB-I via an analysis of the process for dealing with such disputes.

3.2.7 Retention of Ad click Information

It was clarified that ad click information containing IP address information is retained indefinitely, primarily for tax and accounting purposes, legal holds on such data, and improving ad-targeting. The Office advised FB-I that a policy to hold user ad click data indefinitely was completely unacceptable and that FB-I needed to draw up a retention policy as a matter of priority for all data held by FB-I relating to the ads clicked by a user. This matter is dealt with in the Retention Section. FB-I has agreed that it will anonymise[13] ad-click data after a two-year period. Furthermore, FB-I

[13] By "anonymise," FB-I means, for ad-click and search data, FB-I will replace user IDs (UIDs) in logs using a hashing function; for browser cookies (DATR) and IP address, FB-I will remove contents of the browser cookie from the log file and drop the last octet of the IP address

states that the two-year period is necessary 1) to resolve disputes with advertisers, 2) 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), and 3) to improve the overall quality and relevance of ads shown to its users. This is a significant improvement but this Office will keep this matter under active review as we continue to have some doubt about the justification for this period.

3.2.8 Third Party Cookies

The Facebook Data Use Policy envisages the possibility that third party cookies may be dropped on users' machines via advertisements. Facebook's **"Data Use Policy" – Section IV - How Advertising works**[14] states

> *Advertisers sometimes place cookies on your computer in order to make their ads more effective. Learn more at: http://www.networkadvertising.org/managing/opt_out.asp*

.

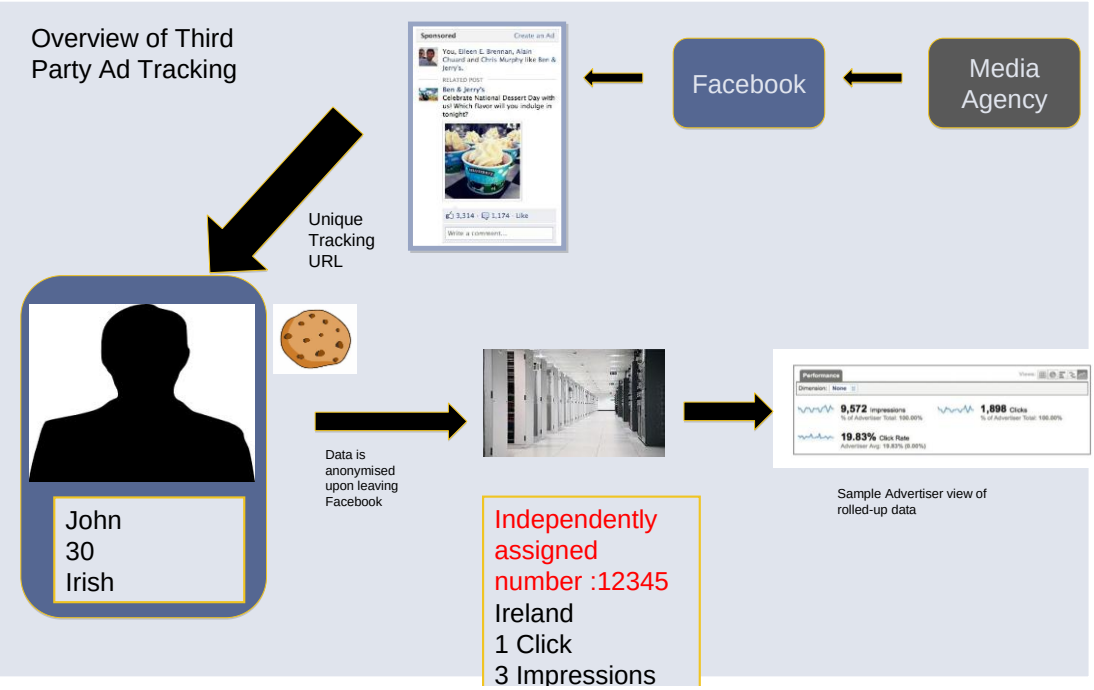
As part of the Audit, we investigated the types of cookies dropped via Facebook ads and the safeguards in place. Facebook's Advertising Guidelines prohibit the use of user data derived from ads served on Facebook (including data derived from cookies) for any purpose off of Facebook.[15]

There are two sets of tags, click tags and view tags, which are permitted in connection with running ads on Facebook. These tags permit the placement of cookies on a user's browser. *FB-I explained that all advertisers may use click tags. FB-I indicated that 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). A more limited subset of advertisers may use view tags. View tags send information to the advertiser when a user views the ad.*

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 measurement, since January 2011, Facebook has implemented a new policy that requires advertisers (or their vendors) that use view tags to be certified by FB-I. FB-I is in the process of instituting this requirement for all such advertisers (or their vendors). FB-I noted that this is an industry-leading practice as most publishers do not impose these restrictions on third-party ad servers. To meet these new requirements, the advertisers (or their vendors) are requested to sign and comply with a 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 advertisers from creating users' profiles or from using any data obtain through Facebook to re-target users with ads outside of Facebook.

FB-I provided an overview of 3rd party ad tracking

[14] http://www.facebook.com/full_data_use_policy
[15] https://www.facebook.com/ad_guidelines.php



FB-I indicates that its Advertising Operations team has systems and models in place to detect ad creatives that contain unauthorized tags. The team is able to identify if the tag comes from a certified vendor or not.

From a technical standpoint, a tracking URL is a random string of numbers. When an advertiser is being billed on third party numbers, Facebook is granted access to the third party ad report to be able to verify the numbers.

3.2.9 Analysis

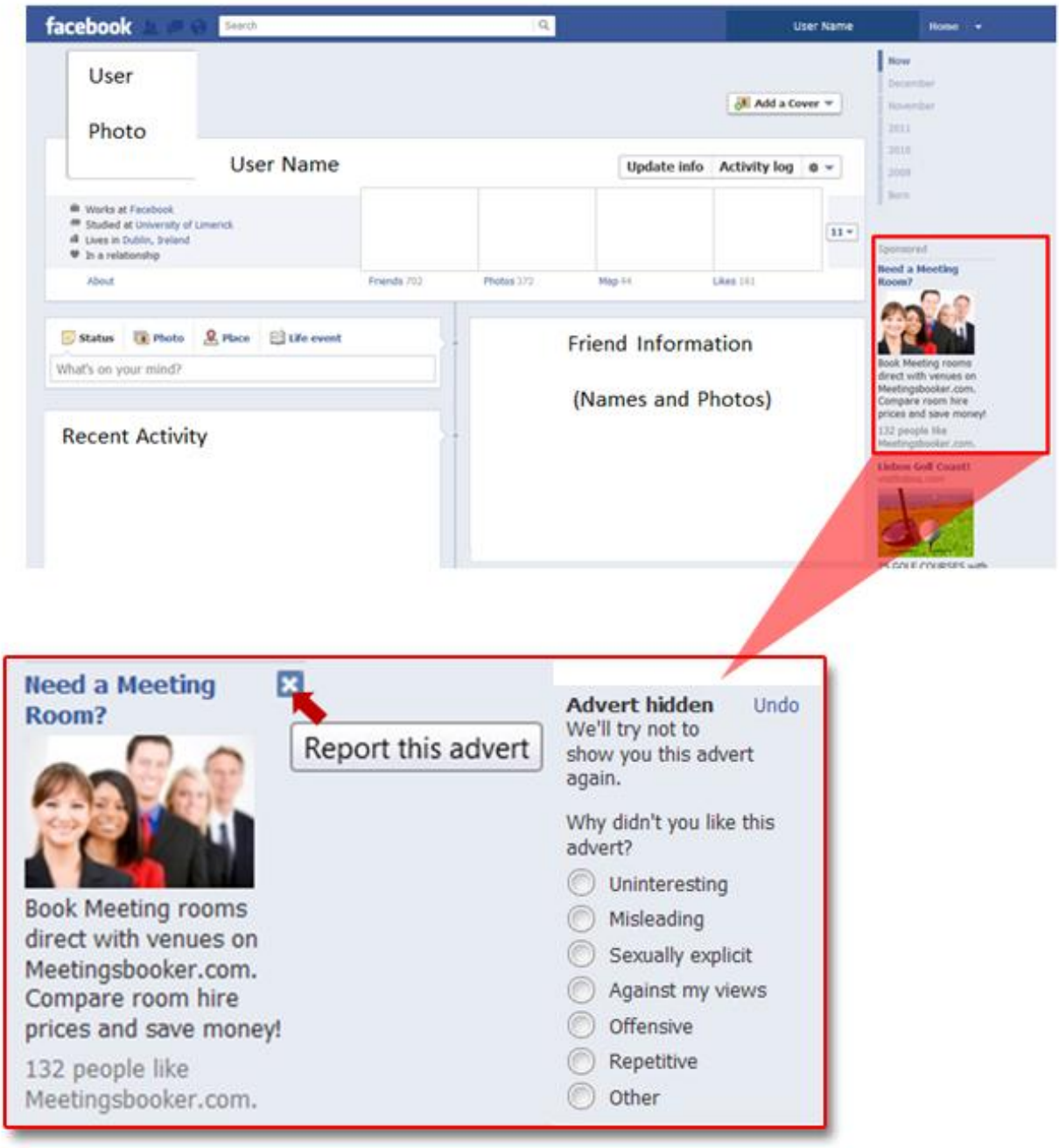
In so far as third parties can place cookies to collect information of Facebook users this issue will remain of interest and concern to this Office and therefore the FB-I approach in this area will be assessed in more detail during the review in July 2012.

3.2.10 Filters and Blocking Mechanisms Provided to Users for Ads

FB-I has indicated to this Office that it has a formal set of procedures in place to provide control to users. See screenshots below.

> *We give people more control over the ads they see than just about any site. If someone doesn't want to see an ad they can click X and indicate a preference not to see that specific ad or not to see ads from that advertiser. You don't have the same control if you walk past a billboard or get shown an ad on TV.*

The availability and use of these features does not appear well known to users and FB-I is therfore asked to take steps to better educate users about the options which they present to control ad content.


facebook
Search
User Name
Home
User
Photo
Add a Cover
User Name
Update info
Activity log
Works at Facebook
Studied at University of Limerick
Lives in Dublin, Ireland
In a relationship
About
Friends 702
Photos 372
Map 44
Likes 161
Status
Photo
Place
Life event
What's on your mind?
Recent Activity
Friend Information
(Names and Photos)
Need a Meeting Room?
Book Meeting rooms direct with venues on Meetingsbooker.com. Compare room hire prices and save money!
132 people like Meetingsbooker.com.
Report this advert
Advert hidden
Undo
We'll try not to show you this advert again.
Why didn't you like this advert?
Uninteresting
Misleading
Sexually explicit
Against my views
Offensive
Repetitive
Other

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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	FB-I will clarify its data use policy to ensure full transparency.	By the end of Q1 2012
	FB-I does not use data collected via social plug-ins for the purpose of targeted advertising	FB-I is taking steps to limit data collection from social plugins, is restricting access to such data and is moving to delete such data according to a retention schedule where collected.	Immediately and routinely thereafter (with the exception of retention for legal hold obligations)
	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	Agreed.	By the end of Q1 2012.
	If, FB-I in future, considers providing individuals' profile pictures and names to third parties for advertising purposes, users would have to	FB-I will enter into discussions with this Office in advance of any plans to introduce such functionality.	n/a

	provide their consent.		
	The current policy of retaining ad-click data indefinitely is unacceptable.	FB-I will move immediately to a 2-year retention period which will be kept under review with a view to further reduction.	Review in July 2012

3.3 Access Requests

3.3.1 Access to Personal data

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[16] what data is held about them and to seek correction or deletion where this may be necessary.

Complaint 10 – Access Requests stated that the data subject lodged a subject access request with FB-I but that the access request resulted in only limited data being provided. It might be noted in this context that FB-I supplied over a thousand pages of data in response to the access request. The complaint outlined 19 categories where FB-I did not provide personal information that it is contended should have been included. The 19 categories cover information in relation to the following:

- Content posted on other's pages
- Videos posted
- Use of 'like' button
- Browser type
- Interaction with advertisements
- Conversation tracking
- Indicates a friendship
- Pictures where tag removed
- Tracking information on use of other websites
- Searches made
- Settings
- Click flows
- Use of 'friend finder'
- Outcomes from matching, face recognition and ad targeting processing
- Use of pictures by face recognition tool
- Data gathered from another's 'synchronisation'
- Relationship with other users
- Reaction of other users to content posted
- 'Invitations' sent and received

The complaint in this area generated a significant amount of interest and as a consequence, the complainant put in place an easy to use template for any person wishing to exercise their right of access to personal data held by FB-I. This resulted in FB-I receiving in excess of 40,000 subject access requests within a matter of weeks. This number of access requests sent to one data controller within this period of time is without precedent in the experience of this Office.

The first issue to be established regarding an organisation's legal responsibility to provide access to personal data is whether the Acts apply to that organisation. As outlined earlier in this report

[16] Section 4 of the Data Protection Acts

FB-I does not in any way dispute its obligation to comply with the Data Protection Acts 1988 & 2003 by virtue of the establishment and operation of FB-I in Ireland. It therefore is seeking to fully comply with all access requests made by users and non-users where FB-I is the data controller for such information[17].

The receipt of in excess of 40,000 access requests within a few weeks would place a strain on the ability of any organisation to provide personal data within 40 days of receipt of the request. There are however a limited number of exemptions contained within the Acts to the requirement to comply with an access request.

In advance of the onsite element of the audit, this Office therefore entered into immediate and detailed discussions with FB-I as to the most appropriate means of providing access to personal data of requesters within as short a time-frame as possible. FB-I had previously devoted extensive engineering time to developing a download tool that would provide access to data that was relatively easy to retrieve and provide. It was agreed that discussions in relation to other types of data held by FB-I would take place during the audit itself and that, once considered, these other categories of data would be added to the download tool or made otherwise available to users.

A significant proportion of the audit was therefore focused on establishing the extent of personal data held by FB-I and whether any of the limited exemptions contained within the Data Protection Acts could be validly claimed by FB-I. We are satisfied that we had full access to all data relating to users and non-users held by FB-I. As outlined elsewhere, the sheer size of Facebook and FB-I and the consequent complexity of user data held is a significant issue. Equally the type of data held by Facebook on individuals is subject to ongoing change in line with the offerings on the site. As an example, the use of "pokes" on the site has declined dramatically as there are now other means for users to communicate with each other. However, as long as such information continues to be stored, it must, in the absence of a statutory exemption, be provided in response to an access request. The issue of retention of information is dealt with elsewhere in the report.

The position of this Office is that, 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. While the complexity and scale of Facebook is an important consideration, it does not, by itself, provide a ground for non-compliance with an access request. This is accepted by FB-I which has approached the obligation to supply personal data in response to access requests in an open and constructive manner. From the perspective of this Office 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. This will also be examined elsewhere in relation to retention.

The attached table details the data which FB-I is now, or will be, providing either via a user's activity log, their profile, user-accessible databases, or additionally in response to an access

[17] Facebook's Terms and Conditions provide that the contractual relationship with users outside of the United States and Canada is with FB-I.

request using the download tool with an indicative date as to when such personal data will be available. FB-I will be making additional data accessible in the download tool beginning in January, with further data to be added at regular intervals, either to the download tool or the activity log. This Office will monitor FB-I's adherence to this schedule and expects that all data will be available in advance of July 2012.

	Available now on User Profile	Available now via Download tool	Will be available from Activity Log	Will be available from Download tool
Profile Information	X	X		
Wall Posts on user profile	X		X	
Photos	X	X	X	
Videos	X	X	X	
Networks	X	X		
Groups	X	X		
Friends	X	X		
Subscriptions		X		
Subscribers	X			
Apps	X			
Likes on Site	X			
News Feed Settings	X			
All comments on your wall posts, photos, videos	X	X	X	
Inbox Messages	X			
Notes	X	X		
IP Addresses	X (limited)			X
Previous Names				X
Account Creation/Deactivation/Reactivation information				X
Encrypted Facial Recognition identifier				X
Verified Mobile numbers for the account				X
Cookie-related information such as browser information, etc.				X
Logins	X (limited)		X	
Wall Posts on other users' profiles and public pages	X		X	
Comments on other users profiles	X		X	
Tags	X		X	
Status Updates	X	X	X	
Pokes	X		X	
Friends' Email addresses (where	X		X	

exposed to you)				
Profile Status Change				X
Searches within Facebook while logged-in			X	
Pages viewed on Facebook while logged-in			X	
Friend Requests/friend invites	X (unless ignored)			X
Event Invites/Acceptances				X
Likes off Site		X	X	
Unlike			X	
Pages admin	X			
Apps Admin	X			

There are very limited categories of information which will not be supplied. As an example, information in relation to a person's passwords, reset passwords, credit card numbers, and verification queries and answers will not be supplied as this information is known to that user and providing it in the activity log or download tool would create a security risk for users if their accounts were breached or if their downloaded data were accessed by a third party. The amount and type of data that may fall into a category that will not be supplied may be affected by any data retention policies or practices as described elsewhere in this Report.

Another category of information relates to abuse reports or employee notes and emails concerning users or former users. From a system architecture perspective it is accepted that it is not immediately possible to supply such information via the means outlined above. There is also a possibility that internal communications may include information, such as staff names and email address and other third-party personal data, that falls outside the scope of a subject access request, and requires significant manual redaction of the communication. Consequently, although FB-I will still accept subject access requests in connection to such types of internal data, FB-I may establish separate and special processes for making a request for such communications.

As indicated elsewhere in this report, this Office conducted a thorough analysis of the use of information gathered from external websites via the social plug-in. This Office is satisfied (for the reasons stated elsewhere) that such information is not associated with the user or used in any way to build a profile of that user. Neither is there any profile formed of non-users which could be attributed to a person on becoming a user.[18]

A number of recommendations are outlined to ensure that this position is maintained, but the issue of access does not arise for such data at this time as it is not related to the user.

3.3.2 FB-I Response

FB-I takes transparency very seriously. We believe the level of transparency we currently provide is substantially greater than any global internet service that is operating at our scale, or even at a

[18] When a non-user joins Facebook, consistent with Facebook's Data Use Policy, Facebook may make recommendations for friend requests to the new user based upon other users who had previously invited the non-user to join Facebook at the email registered at account creation.

scale an order of magnitude smaller than ours. We believe that we have innovated extraordinary new tools to help users review and understand the personal data in our possession and we are committed to continue to innovate to remain transparency leaders. We are dedicated to provide our users the best experience on the platform and the easiest way to exercise their rights. We invest significant engineering time and resources to develop best in class tools for users to easily access and manage their own data.

First and foremost, it is important to recognize that Facebook users can easily review, correct, delete and download the vast majority of their personal data simply by logging into their accounts. FB-I seeks to provide our users with upfront access to as much of their personal data as possible, without requiring them to make formal subject access requests. Easy access by users to their personal data is something we have designed into the Facebook service. Our Data Use Policy explains the categories of data being processed, the purposes of the processing and the categories of recipients to whom the data are or may be disclosed.

Second, we have recently created an innovative tool ("Download Your Information") which allows users to download most of the content they have previously uploaded onto Facebook in a single file.

Finally, FB-I has recently announced the addition of a new transparency tool by creating a soon-to-be-launched feature called "Activity Log." The Activity Log will provide users with even more of their personal data simply by logging into their accounts.

We recognize, however, that we are innovating in an area where there is little precedent or practice. The 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.

Previously, for users who required personal information which may not be available on the site, we had a specific contact form that could be used to request their personal data. Given the volume of requests we received over the course of one month, we found it disproportionately burdensome to continue to respond to access requests manually. We have therefore been working towards an automated, self-service option, which will satisfy our users.

FB-I is committed to provide data subjects with the personal data we hold and to make such data easily accessible on our site through a variety of means: the download tool, user-accessible database, the new "Activity Log", and the user's own account. FB-I has agreed with the DPC to provide the additional categories of data listed by the DPC above. FB-I emphasizes, however, that to make all of this personal data available to users will take significant engineering efforts and resources. FB-I has agreed to provide additional data in the download tool in January and to make substantial additional fields of data accessible no later than the end of the first quarter 2012. The remaining data will be provided via an enhanced activity log within Timeline as soon as the

necessary engineering work which is ongoing is completed. We will keep in ongoing contact with the DPC to ensure this timescale is met.

3.3.3 Analysis

Significant progress has taken place in terms of FB-I's understanding of the need to comply with requests for data in a timely and comprehensive manner. Importantly, the audit however has established an important principle of transparency as follows:

> *Transparency is a core value of FB-I. FB-I believes that our users are entitled to have easy and effective access to their personal information. To achieve this goal, we shall endeavour not to unnecessarily use or retain the personal data of users where such data cannot be made easily available to the user.*

We are satisfied that FB-I is working actively to achieve this objective and therefore recommend that it maintains the principle of transparency outlined above. The above matters and the response of FB-I to individual requests for personal data will be kept under full review by this Office specifically to ensure that the timescales outlined for the provision of data are met. This issue will be revisited in the context of specific complaints received and the audit review to be conducted in July 2012.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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	FB-I will fully comply with the right of access to personal data, as outlined in the schedule above. It has additionally committed to a key transparency principle that users are entitled to have easy and effective access to their personal information.	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.

3.4 Retention

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. We have also found that data controllers as a class have not adequately met their obligations in this regard and the consequence is inappropriate processing and disclosure of personal data that should no longer be held by a data controller. In Facebook's case, as acknowledged earlier in this report it is still a relatively new company but obviously one that holds a large amount of data via its some 800 million users. That FB-I should have work to do on meeting its retention obligations was therefore perhaps not surprising.

A number of complaints received from Europe-v-Facebook also addressed the issue of retention in specific instances. While those complaints touched on other issues related to fair processing, this section will only examine the retention aspects.

3.4.1 Complaint 1 – Pokes

In the complaint it was stated that a 'poke' is a type of short message sent from one Facebook user to another. If the user to whom the 'poke' is sent wishes to remove that 'poke', they may click on a small 'x' provided next to it. The complainant stated that while Facebook allows for this removal of old pokes, they were not, in fact, being deleted.

As part of an access request made to Facebook, the complainant was provided with a copy of all pokes ever sent or received going back over a 2 year period to the time when he first set up his Facebook account. From the data provided, the complainant contended that Facebook marks 'removed' pokes as 'viewed' but is not, in fact, deleting them.

3.4.2 Complaint 3 – Tagging

Complaint 11 – Removal of Tags

The complaint stated that Friends on Facebook have the facility to 'tag' photos of another user (friend) and display them on their Facebook page and within the 'news feed' section. The complainant contends that if the user decides to remove a 'tag' it is not deleted and is retained in the background by Facebook. The broader data protection compliance of tagging is considered elsewhere in the report.

Both the 'tagged' user and the 'tagging' user have the option to subsequently remove the 'tag' if they wish. However, the complainant contended that removing the tag is not deleting the tag data and that Facebook is not being transparent in terms of informing users on the retention of this information following the use of the 'remove tag' option.

3.4.3 Complaint 14 - Removed Friends

In addition to being able to 'find' and 'add' friends, Facebook users also have the option of removing friends from their friends list.

The complainant stated that, in response to his access request to Facebook, he was provided with a list of people he had previously removed from his friends list. The complainant stated that he presumed these names to have been deleted at the time he used the remove option and that some of the names would have been removed up to 3 years ago.

The complainant contended that there is no justification or user consent for the retention of this data and considered that Facebook was not transparent in terms of informing users on the retention of the information.

3.4.4 Complaint 21 – Groups

Facebook allows users to add friends to groups, a Facebook feature that allows users to form communities around shared interests, among other things. The issue raised in the complaint is that a user can be added to a Group without the user's prior consent. The complainant contended that a user may be unaware that they have been added to a Group and that Groups can be 'public' meaning anyone can see that the user is a group member.

The complainant indicated that a user can remove himself from a Group, but only after he has been made aware that he was added as a group member in the first place. The complainant contended that, even when the user has removed himself, Facebook retains the data that links the user with the Group.

3.4.5 Complaint 5 – Deleted Posts

The complaint indicates that Facebook provides a facility whereby a user can delete items such as old posts from their Facebook page. The complainant stated that he used the 'remove post' option, applying it to virtually all posts he had made going back over a three year period. When he completed this exercise he indicated that a message at the foot of his Facebook page stated that there were no more posts to show.

On foot of the access request made by the complainant to Facebook, the information he received in response included a random number of items, including posts, which he stated were deleted by him. He contended that some of his original posts must have been deleted, but some – going back as far as three years ago - were retained in the background by Facebook.

The complainant considered that there was no legitimate purpose for the retention of data which a user might reasonably expect to have been deleted. In addition, he stated that there was no transparent notice provided by Facebook to inform users that data, which they would have presumed to have been deleted, had been retained by Facebook.

3.4.6 Analysis

These are issues which require careful analysis as they are about transparency and control for the user. At present, the information provided to users in relation to what actually happens to deleted or removed content, such as friend requests received (not sent as what happens to those

is the personal data of the recipient primarily), pokes, removed groups and tags, and deleted posts and messages could be improved. This is accepted by FB-I and this will be reflected in an updated Data Use Policy. From the control perspective, at present there is no facility for a user to delete friend requests, pokes and tags. FB-I noted that it has already made changes to its service to improve visibility to users of data that previously was not visible. Facebook's new profile, called "Timeline", has a feature called "Activity Log," on which many of the user's actions around Facebook can now be viewed privately by the user. Since "Activity log" is only visible to the user, FB-I has proposed to use this feature as a means for users to access, review and delete their own data. Building the Activity Log was, according to FB-I, an involved and lengthy engineering task, but FB-I is committed to add further data to the log and to give users the ability, where appropriate, to delete, if not all, then most of the data. However, as stated in the Section on Access, "transparency is a core value of FB-I. FB-I believes that our users are entitled to have easy and effective access to their personal information. To achieve this goal, we shall endeavour not to unnecessarily use or retain the personal data of users where such data cannot be made easily available to the user." FB-I has also in this respect undertaken a policy of allowing users maximum control over their data and to the maximum extent possible will be extending an ability to delete on a per item basis individual data items. Given the size of the engineering task, FB-I has agreed to begin working on the project during Quarter 1 of 2012. FB-I has committed to showing demonstrable progress by our July 2012 review.

While it is accepted that the adding of users to Groups is confined to their friends, it is the case that a small minority of users on Facebook have an extensive network of friends in many cases in excess of 500. While that, of course, is a matter of personal choice it does bring with it a risk that a person could be added to a Group with an ethos that might offend them or others and for the time that they appear as such this could be a cause of significant embarrassment.

Additionally, even where a user leaves a Group, this fact is retained by Facebook at present to ensure they are not added to the Group again. This is similar to the complaints in relation to pokes, friend requests and tags in that essentially it is a matter of transparency and control. Additionally, to address this Office's concern that the current operation of the Groups product may in certain situations work to imply that a user shares the views of a particular group before the user has an opportunity to leave the group in question, FB-I has also agreed to review and revise the news story that is created when a user's friend invites the user to join a group to avoid the suggestion that the user has in fact joined the group, until the user has been given an opportunity to leave the group. FB-I has also agreed to introduce a mechanism to identify, when viewing the group itself, which listed users are members, as compared to which users have merely been invited. The user status will change from "invited to the group" to "member" only after the user visits the group for the first time. The user will be able to check the content of the group and make a decision about whether or not he/she wants to be associated with this group. If a user does not want to be part of the group, he/she will be able to click on the option to leave the group.

FB-I's response on these complaints highlighted that it retained such information for what it termed various important purposes to provide the best possible experience to users. For example, it stated it needs to save removed pokes in order to assist in identifying instances of bullying and harassment; FB-I saves rejected friend requests so that the same user cannot continue to send friend requests; FB-I uses removed friends data to ensure that the removed friend isn't surfaced as

a friend suggestion to the user; and FB-I uses removed tags to prevent the user from being re-tagged in the photo. FB-I has pointed out that this has been developed based on the comments and requests from their users. FB-I points to its Data Use Policy to demonstrate that it is transparent about the purposes for which it uses the data it receives.

FB-I explained that content that is deleted is immediately removed from the site and can no longer be viewed by third parties, and that it then begins the process of deleting the content from all of the places it exists on their servers. This process can take up to 90 days, as is disclosed in the Data Use Policy and described in the technical analysis report and the section on deletion in this report. In response to the random posts provided in the subject access request, FB-I stated that some posts had not yet been purged by the time a response to the request had issued and that some information may remain within servers for up to 90 days.

The broader issue of how the deletion process operates within Facebook is dealt with separately in this report. This analysis is confined to the continued justification to hold post data which a user might consider was deleted or for which FB-I cannot identify an evidence based justification to continue to hold. This Office is satisfied that FB-I does delete old posts from a user's own Profiles and from other user's Profiles which are marked for removal. The appearance of these in the response to the complainant is that they were only marked for deletion at the beginning of July of this year approx 12 days before the date of the access request. Therefore regardless of the date on which the post was made the relevant date for deletion was the date on which the deletion request was made. However, as indicated above, FB-I has agreed to provide greater transparency and control over posts to users in their Activity Log as part of Timeline and this will allow a user a greater opportunity to mark for deletion any such posts.

FB-I explained that it operates large, distributed computing systems, where information necessarily is stored in many places at once. For example, FB-I operates multiple data centres in different geographic areas, each of which stores copies of the information in Facebook's databases. Having data centres located near the people who use Facebook helps FB-I provide access to Facebook without long delays. Using multiple data centres also provides redundancy, ensuring that Facebook will continue to function even if a single data centre is receiving an unusually high amount of traffic, experiences a network problem, or becomes unavailable for another reason. FB-I also stores emergency backups of Facebook data in multiple locations to protect against data loss.

The consequence of using distributed architecture is that information users post on Facebook is often stored in multiple physical locations at once. This creates a significant engineering challenge because, when FB-I deletes information, it often has to do this not just in one place but in multiple locations. FB-I states that it describes this process in its online Statement of Rights and Responsibilities, which says, *"When you delete [content you post on Facebook], it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others)."*

Given the complexity of building deletion mechanisms that will work across its technical environment in a manner consistent with its policies and commitments, FB-I has a multidisciplinary group of experts within the group of Facebook companies that have been and are

working to address these technical challenges. FB-I expressed that it is committed to continually working to identify changes in its procedures to maintain and increase their effectiveness, even as its service evolves over time.

3.4.7 Complaint 7 – Messages

The complainant stated that Facebook provides users with a messaging service whereby users may send instant messages to other users who are online. It should be highlighted that this messaging service is now expanded to include the sending and receipt of emails using a Facebook domain. The complainant indicated that it is also possible to delete these instant messages if the user so chooses by clicking on the 'delete messages' option provided. However, the complainant contended that the act of hitting the delete button provided merely removes the message from view and does not in fact, delete it. The complainant stated that information regarding the non-deletion of this data is difficult to find within the Facebook Data Use Policy.

The complainant considered that Facebook was in contravention of data protection legislation in that the user, having clicked 'delete messages' has not consented to the message data being retained. In addition, he considered that if both users involved in an instant message have chosen to delete it, Facebook has no legitimate purpose for retaining this data.

3.4.8 Analysis

The issue of the retention of messages appears to be well understood by the complainant. If the message remains in either the sent box of the sender or the inbox of the recipient, then it could not be expected that the message would be deleted by FB-I. However, if it is removed from both the sender's box and the recipients' boxes, then the continued justification for holding such a message is questionable. FB-I states that its policy and practice is to delete a message after the last person user deletes the message. This Office is satisfied with this best practice approach. This was not verified during the course of the audit but will be confirmed during the review.

3.4.9 Complaint 15 – Excessive Processing

This complaint covers issues raised in a number of other complaints. The complainant made a general point in relation to the amount of data being retained and processed by FB-I and contends that the retention of so much data is excessive and a security risk.

The complainant contended that users should have 'real' options in terms of deleting their own personal data (pokes, tags, etc.) which users may have removed and presumed to have been deleted but, as he alleges in his complaints, are in fact retained in the background. The complainant considered the amount of data Facebook holds and processes to be excessive.

FB-I, inter alia, pointed to the worldwide popularity of the platform and contended that the fact that Facebook processes the data of a very large number of people does not in itself mean that that processing is excessive. Furthermore, FB-I noted that processing is excessive where it was unnecessary, not simply where it justifiably involved a large amount of personal data.

3.4.10 Analysis

This complaint needs to be considered in the context of the specific other complaints listed above. There is no specific information provided that would lead to a conclusion generally in the context of this complaint that FB-I is engaged in excessive data processing. However, more generally

within this section of the Report we return to this issue based on information accessed and examined during the onsite element of the audit.

3.4.11 Complaint 17 – Like Button

The complainant states that when a user visits a website which contains a 'social plug in' – the Like button – the following information is being recorded: date, time, URL, IP address, browser and operating system information. The complainant considers that the information is being collected unfairly and is excessive and allows Facebook to track user movements across the web.

Although there are detailed data retention issues, the use of social plug-in data will be considered separately in this Report as a specific item.

3.4.12 General Findings on Retention

A recurring theme in audits conducted by this Office is the ongoing challenge for data controllers to meet the requirement in practice to delete personal data once it has served the basic purpose for which it was collected. Our audit of FB-I has demonstrated this once again and as a consequence a significant portion of the audit was focused on this issue across many fronts. At the outset it is perhaps worth recalling that Facebook Inc. remains a relatively young company only formed in 2004 and the majority of its user base only joining in recent years. In addition, FB-I was established as the European headquarters and came unambiguously under the jurisdiction of Irish data protection law only in late 2010. Therefore, like any start-up company, requirements in relation to retention of personal data were not an immediate priority. Additionally, FB-I's business requires in many cases the retention of personal data in order to provide the services its users expect when they join Facebook. FB-I therefore has indicated its commitment to increasing visibility and control over data it needs to keep to support its users. As well, FB-I has confirmed and recognised the need to 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.

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.

Social plugin impression log data and cookies

FB-I has developed a new retention policy with respect to impression log data and cookies:

- *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 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.

Search data
FB-I has developed a policy that it will anonymise all search data on the site within six months.

Ad-click data
FB-I has developed a policy that it will anonymise ad click data after 2 years.

Login Information
FB-I retains information in relation to the login activity of users. FB-I reports that it does so for security purposes, and this is examined separately in this report in the Security section. This includes the date, time, IP address used, browser, operating system information and security cookie information from every such login by a user. At its most basic level, we would consider that 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. FB-I has undertaken to enhance the information available in this regard.

We are satisfied that all such recording and retention of information is for security related and fraud investigative purposes. We found no evidence, from a very extensive examination of code, logging and queries served to the logged data that the information gathered was used for any advertising, predictive or user profiling purposes. Access to the information was confined to the security team, limited staff members in user operations and to the Facebook Credits suspicious payments investigation team. The operation of Facebook Credits is dealt with separately in this Report.

The question to be assessed therefore is how much user login information is sufficient for FB-I to meet its objectives to secure its system from bad actors. FB-I informed this Office in the course of the audit that there are approx 600,000 attempts made each day to illegally access or take over user accounts on Facebook. This is an extraordinary figure and reflects the size and significance of Facebook as a means of communication. It is therefore necessary to take due account of such activity when considering this issue. FB-I has provided to this Office an appropriate evidence base to justify the retention period. The continuing justification for this period will be kept under continuous assessment and will be specifically re-assessed in our July 2012 review.

Issues also arise in relation to the retention of information via Cookies and IP address of persons who have only visited Facebook but not joined. FB-I have provided evidence to this Office that a significant proportion of persons prior to seeking to maliciously access the site or an account will have previously visited the site and that the possibility of correlating such activity is important in securing user information. This is accepted. However, the proportion of persons who will engage in such activity markedly declines with the passage of time and cannot be used as a justification for the continued storage of security cookie information for all users when such information would be of no assistance in identifying unusual activity related to their account or Facebook generally.

It would appear therefore that a combination of approaches which limit information stored taking account of time and numbers of log-ons best meets the criteria for balance in this area. This Office has agreed such an approach with FB-I but the precise details will not be set out here as to do so would provide a means to undermine security.

We are satisfied that FB-I does not use or seek to use any information that might identify a person who has never visited Facebook that it may have collected inadvertently via the social plug-in. As previously stated this issue is separately assessed in this Report.

Search within Facebook
Additionally in relation to the above categories of information, while the user will have a possibility to manage such information via the activity log, as this may entail extensive administration on the part of the user which would tend to discourage such activity, FB-I has agreed to effectively anonymise all such information after 180 days even if the user has not chosen to do so. This will also have the effect of removing such information from the activity log.

Deletion of Inactive/Deactivated Accounts
The above improvements will provide significant control to users over each item of personal data held on them by FB-I. Now that Facebook has matured to an established company there remains an issue to be addressed in relation to how long Facebook 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 Facebook 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 Facebook. This therefore is a complex issue and one on which this Office intends to have further discussions with FB-I.

The complexity of an information society service such as Facebook 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.

Deletion of Data from Incomplete Registration

As outlined in the Privacy Policy/Data Use Section, a person registering with Facebook is presented with links to the Privacy Policy and Statement of Rights and Responsibilities on the second screen of the process and are deemed to have consented having entered the captcha code on that screen. On the first screen of the process prior to having the ability to read these policies (a potential user can also read them at present from the bottom of the facebook.com page without having to go through the registration process) name, email address, gender and date of birth must be entered. Therefore we sought to establish what happens to the data entered on the first screen if the user chooses to cancel their account registration for any reason.

We have established that the user may be sent reminder emails during a 30-day period, asking them if they want to return to complete the registration process. After 30 days, if the user has not completed the registration process, an automated process will delete the information provided. The code of this automated process was reviewed and confirmed to operate as specified, deleting all information stored when the user filled in the first page of the registration after this time.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I will comply with this recommendation in an updated Data use Policy.	By the end of Q1 2012.
	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.	FB-I will phase in such transparency and control to users on a regular basis.	FB-I has agreed to begin working on the project during Q1 of 2012. FB-I has committed to showing demonstrable progress by our July 2012 review. This time-scale takes account of the size of the engineering task.
	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 recorded 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 recorded as being a member until s/he visits the group and will be given an easy method of leaving the group	By the end of Q1 2012.

	Personal data collected must be deleted when the purpose for which it was collected has ceased	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	Immediate and ongoing, subject to any legal holds placed on the data by civil litigation or law enforcement. The continuing justification for these periods will be kept under continuous assessment and will be specifically re-assessed in our July 2012 review.

		visits a website that includes a social plugin. 3. anonymise all search data on the site within six months 4. anonymise all ad click data after 2 years 5. significantly shorten the retention period for log-in information to a period which was agreed with this Office	
	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.	FB-I will provide additional information in a revised Data Use Policy	By the end of Q1 2012.
	We have confirmed that data entered on an incomplete registration is deleted after 30 days		
	Data held in relation to inactive or de-activated accounts must be subject to a retention policy	FB-I will work with this Office to identify an acceptable retention period	July 2012.

3.5 Cookies / Social Plug-ins

In advance of the audit there was significant public comment and discussion in relation to the collection of information by Facebook when individuals visit websites which contain a Facebook social plug-in, e.g. a Like Button. Facebook, like almost every website, also drops cookies (text containing a piece of information) when a person visits Facebook.com. This is a standard practice on the internet.

This issue was examined closely with FB-I during the course of the audit to establish precisely what information is collected, in what circumstances and for what purposes. The results of the detailed technical analysis are contained in section 6 of Appendix 1. This matter is also dealt with in the advertising and retention sections.

By way of background, social plugins (the "Like" button) are a feature provided by Facebook to website owners, according to Facebook to allow the owners of websites to provide a customised browsing experience for Facebook users. The social plugin allows users to see 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, recommended, or commented upon on the site. If a logged-in user clicks on a social plugin, the button turns darker to indicate the user has clicked it. Back on Facebook, a story will appear on the user's Timeline and may appear in the Ticker and/or News Feed, just as if the user liked something on Facebook. Equally, as outlined in the Advertising Section, a user who is not logged in can click the "like" button and be prompted to log in to see personalised content and interact with the plugin.

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. This is a standard way that content from different publishers is loaded to a website. When a user visits one of these sites, the Facebook iframe can recognize if the user is logged into Facebook. If the user is logged in, the website will show personalized content within the plugin as if the user were on Facebook.com directly.

We have confirmed that the content of the social plugin iframe is delivered directly to the web browser from Facebook and the website on which the social plugin is hosted has no visibility of the content of the social plugin delivered.

The type of information collected by Facebook varies depending on whether the person is (i) a logged-in Facebook user, (ii) a logged-out Facebook user, (iii) not a Facebook user and never visited Facebook.com and (iv) not a Facebook user and visited Facebook.com within the last two years but not cleared their cookies in the meantime.

3.5.1 Non-Facebook Users

For a non-Facebook user who has never visited Facebook, no cookies are sent either to or by Facebook when a user visits websites containing social plugins. The user's IP Address is collected in order to deliver the iframe as above.

When a non-Facebook user visits www.facebook.com, three cookies are set by Facebook. Two are session cookies and one is a cookie set for two years for security reasons as outlined elsewhere. If this non-user does not clear their cookies and visits a website with a social plug-in, four cookies will be set by Facebook when delivering the plug-in to their browser. An explanation of the purpose of these cookies is outlined in the cookie analysis section of the Technical Analysis Report (appendix 1).

3.5.2 Facebook Users

There are some small distinctions between the cookie information sent when a logged-in or logged-out user browses to a website with a social plug-in. These are outlined in more detail in Sections 6.4.1 & 6.4.2 of the Technical Analysis Report.

The Datr cookie identifies the web browser used to connect to Facebook. This cookie is used for security, among other purposes. For example, this cookie is also used to underpin login notifications and approvals.

The lifetime of this cookie is currently two years. We expect Facebook to examine shortening this period. However, for the reasons outlined in the Security Section we are not raising any concern over the use of this cookie. Our focus is on the use of the data collected and the need to implement a very short retention period where the data collected is from social plug-ins on external websites.

A second notable cookie is used to manage how the login page is presented to the user. Several pieces of information are encoded within this cookie, as described here:

- 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) in most cases.

- A steady flow of cookies beginning with _e_ are transmitted between the user's web browser and Facebook. These cookies contain performance-related information pertaining to the user's actions on the website. The cookies are session cookies and the values of these cookies are set by the user's browser and unset by the Facebook servers on virtually every request as described in Section 6.6 of the Technical Analysis Report at Appendix 1.

3.5.3 Non-Cookie Information

Aside from the cookie information described in the previous section, the relevant information from a data protection perspective that is sent by an individual's browser to Facebook when social plugins are loaded is:

- Time and date of request
    - The time and date that the Facebook server received the request.
- Browser IP addresses

- 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[19].

3.5.4 Logging of Information

The structure of Facebook log entries was reviewed as well as the code that performs logging. Access was sought and provided to the log entries, the code used to query the entries and the queries made to the logs and we were satisfied that no access was made to any information that could be considered to be personal data in the logged information for advertising or profiling purposes.

Tests were also performed to attempt to establish whether or not the act of a logged-in Facebook user simply browsing to pages that have social plugins (as opposed to clicking the "Like" button) would influence the advertising that the user is presented with. An affirmative result would strongly indicate that Facebook were using browsing activity to target advertising, which it is claimed is not the case.

No correlation with browsing activity was identified.

This is an issue which was also the subject of complaint from Europe-v-Facebook, **Complaint 17** – Like Button. The complainant stated that when a user visits a website which contains a 'social plug in' – the Like button – the following information is being recorded: date, time, URL, IP address, browser and operating system information. The complainant considers that the information is being collected unfairly and is excessive and allows Facebook to track user movements across the web.

FB-I Response

FB-I stated that it has not designed its systems to track user and non user browsing activity and that users have provided consent for the processing of data. FB-I contended that it provides 'exhaustive' information in relation to the use of 'social plug ins'

> *When you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time, and other browser-related information.*
>
> *If you don't have a Facebook account and visit a website with the Like button or another social plugin, your browser sends us a more limited set of information. For example, because you're not a Facebook user, we don't receive a user ID. We do receive the web page you're visiting, the date and time, and other browser-related information. We record this information for a limited amount of time to help us improve our products.*

[19] Certain scenarios exist, notably the use of NAT (Network Address Translation) or the use of a web proxy, where the browser is not making a direct TCP/IP connection to Facebook. In these cases the IP address received by Facebook will not necessarily be the same IP address as that of the browser's PC.

3.5.5 Active Cookie Management

An obvious concern for this Office in examining FB-I's use of cookies is the unsettled questions that recur about the purposes to which FB-I's puts the data received from cookies and the need to minimise the collection in the first place. We therefore sought concrete measures to minimise the possibility of the future collection of unsought data. The Facebook security team have demonstrated a recently improved feature for proactive management of browser cookie state, known as "Cookie Monster". The code of this feature was reviewed and confirmed to operate as described in the Technical Analysis Report.

FB-I response

Historically, cookies only intended for logged in users were cleared by Facebook on logout. There were two challenges presented by this: (a) Facebook engineers needed to specify the behaviour of the cookie in multiple locations in the codebase, and (b) if a user was logged out by means other than explicitly logging out, the cookies would not be cleared (e.g., a user might be logged out by manually clearing one of their cookies, by quitting their browser, or due to a bug in the browser, a browser plugin, or Facebook itself). In response to these issues, Facebook extended an existing cookie management framework to make it more reliable and comprehensive. For example, on any request where Facebook can determine that a user is not logged in, any cookies present in the request but only intended for logged in users will be cleared. On some requests, this is not possible, but it is attempted on every request. As a result, in practice, cookies only intended for logged in users should be reliably cleared shortly after the user is logged out regardless of how the user becomes logged out. This cookie management framework also enforces other similar policies about cookies (e.g., which cookies are only sent over https requests and which cookies are visible to Javascript executing in the browser).

It can be assumed that this framework will serve to assist Facebook in combating the collection of excessive information via cookies which were initially intended for another more limited purpose. We will keep this area under review and will re-examine the operation of the framework in July 2012.

3.5.6 Analysis

Facebook, as outlined repeatedly in this report, is perhaps the most complex technical environment on the internet. The use of social plug-ins on several million websites has added to that complexity and increased exponentially the data which Facebook receives in order to serve those plugins to every browser that visits those websites. FB-I strongly asserts that it has not designed its systems to use any data derived from the serving of the social plug-ins to profile either users or non-users for when they join. In the case of users it is the position of FB-I that they already have a rich source of information provided by the users themselves via their own profiles, their likes, their interests, etc. to have no desire to use such information. However, undertakings in relation to the relative utility of such information are not sufficient of themselves to allay fears as in the case of Facebook users whether logged-in or not Facebook has a direct means, if it chose to do so, to associate the social plug-in browsing data with the user. It also has a means to build a profile of a non-user who has visited Facebook.com and associate it with them in the event that they do join.

Our task therefore was to satisfy ourselves that no such use was made of the collected data. We are satisfied on this point. Secondly given the vast amount of data held we also had to verify that

the data collected was not queried or otherwise accessed for any purpose other than for site quality etc.

FB-I has confirmed to this Office that, as part of its commitments described below it will be amending its data retention policy for social plugin impression logs to provide enhanced protection to the information of users and non-users. Specifically, under its revised policy, for people who are not Facebook users or who are Facebook users in a logged out state, 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. In addition, 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. These combined measures ensure that FB-I retains information stored in social plugin impression logs for a minimal period of time.

While this Office acknowledges the technical and practical challenges with respect to deleting social plugin impression data, including current issues resulting from litigation in the United States, it is not appropriate for Facebook to hold such information other than for a very short period for very limited purposes.

In this respect, we are aware that from time to time class action or other litigation is filed against Facebook that can require the company to retain data for purposes of such litigation, including social plugin data. In addition, FB-I informed this Office that in August of this year, it discovered social plugin impression data that should have been anonymised or deleted had not been. It stated that as soon as it became aware of this situation, it began to implement a technical process to delete such information. Substantial progress in deleting the data had been made when retention of social plugin impression data became required for litigation purposes.

After a detailed review of FB-I's technical systems for data deletion, we are satisfied that FB-I is committed to building the infrastructure necessary to comply with its new, enhanced, data retention policies. FB-I has undertaken to review the technical systems used specifically for the deletion of social plugin log records and report back to this Office on their current effectiveness and how they will be amended to support this change to its data retention policy. We have asked FB-I to put in place measures to implement its new retention commitments for social plugin impression data by July 2012.

This Office welcomes this new approach and given the sensitivity of this issue we will be verifying deletion of the first batch in line with this commitment as soon as it happens.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.		
	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	Impression data received from social plugins will be anonymised within 10 days for logged-out and non-users and deleted within 90 days, and for logged-in users, the data will be aggregated and/or anonymised in 90 days.	Immediately and to be verified by this Office subject to any legal holds placed on the data by civil litigation

3.6. Third-Party Apps

3.6.1 Background

Facebook provides an application platform to allow third party developers to build applications that integrate with the Facebook Platform[20]. Facebook also provides development platforms for integration with other websites (e.g. social plugins which are discussed separately in this report) and integration with mobile applications.

The use of third party applications is an issue which our colleagues in the Nordic countries[21] and Canada have examined extensively in previous investigations. It was also an issue which formed part of the complaints examined by the Federal Trade Commission (FTC) in its recent investigation which was settled and announced on 29 November 2011[22]. Among the issues examined by the FTC was a complaint that Facebook was passing user data to third party applications via the unique user id. Facebook in response to the FTC indicated that it had resolved that particular issue.

3.6.2 Complaint 13 – Applications

The role and use of third party applications was also an issue outlined in the complaints received from Europe-v-Facebook.org. This complaint pointed out that Facebook users are offered the option of using third party applications – games, quizzes, etc. – which can be accessed via the Facebook platform. It contended that Facebook allows third party applications access to the user data it holds, including the personal data of 'friends' of the user.

The complainant suggests that Facebook does not take enough responsibility in ensuring that these third party organisations have a privacy policy (this was outlined in Complaint 12 also) and does not notify users in a case where a third party has no privacy policy.

The complainant considered there to be a lack of informed user consent when accessing a third party application.

3.6.3 Norwegian Consumer Council

In the complaints submitted by it on this issue (see Appendix 2), the Council indicates that when a Facebook user signs up to a third party application that the user's data is provided to the application. The Council contends, from information collected from a survey it carried out, that "many people believe the applications to be part of Facebook and they are therefore not even aware that they are interacting with a third party". The Council also considers that many of the terms and conditions of third party applications are complex or unclear.

The Council stated that a user signing up to a third party application must accept the application's terms and conditions in order to use the service. The Council raised issues with specific third party application developers.

[20] https://developers.facebook.com/
[21] http://www.datatilsynet.no/upload/Dokumenter/utredninger%20av%20Datatilsynet/Microsoft%20Word%20-%2011-00643-5%20Part%20II%20-%20Questions%20to%20Facebook%20from%20Nordic%20DPA.pdf
[22] http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf

Facebook considered its information regarding third party applications to be clear. In its Statement of Rights and Responsibilities, Facebook states that

> *When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information.*

It also highlighted information contained within its Data Use Policy titled *"Sharing with other websites and applications."* This section describes platform *("About Platform"*), provides information on how to control information that is shared with applications (both when you use platform and when your friends do), and includes other relevant information as well.

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

Given the prominence of third-party applications on Facebook, a specific focus was placed on examining their interplay with Facebook. A number of meetings were held with the relevant teams based in Dublin as outlined below and a detailed examination was undertaken of the code available to third party developers to access user information. A key focus in this regard was to verify that it was not possible for an application to access personal data over and above that to which an individual gives their consent or access personal data of any other user beyond that enabled by the relevant settings.

3.6.4 Developer Relations

In addition to a technical examination, it was felt appropriate to meet with the individual teams responsible for managing third party applications. A team of FB-I staff known as "Developer Relations", offer developer support to external developers who are developing third party applications and plug-ins using tools and API code available on the 'Facebook Platform'. A reciprocal team is currently being established in Menlo Park, California to mirror the functions of the existing team in Ireland and allow for the provision of 24 hour development support cover.

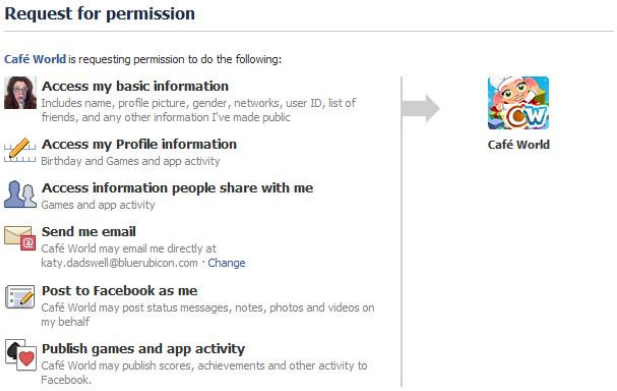
All third party applications and developers are external to Facebook and range from an individual building an app as a hobby to a professional developer or large organisation building a range of apps connected to certain products or campaigns, including for example gaming apps in which users must pay for premium content. The Developer Relations team generally focus on bug fixing, testing and code amendment in relation to the Facebook APIs. We examined with Platform Operations a number of reports received regarding bugs and inspected the data in relation to developers that are stored and used. No particular issues in this regard arose.

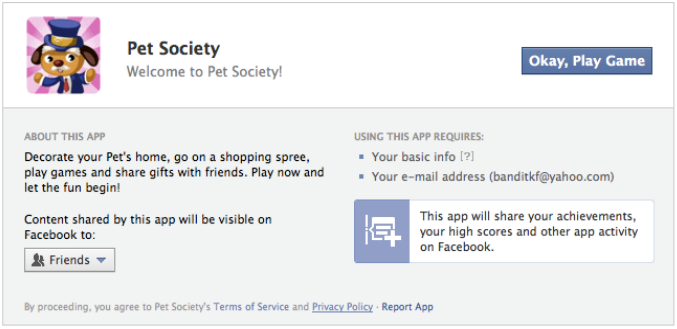
3.6.5 Platform Operations

The role of Platform Operations is to enforce Facebook's Platform Policy, interacting with developers of third party apps and developers using the social graph, i.e., social plugins, to ensure adherence to Platform Policy. An examination was conducted of the work queues of the Platform Operations Team. It was noted that Facebook has now introduced a number of automated tools, developed in Dublin, to proactively and automatically identify and disable applications engaged in inappropriate activity such as spamming friends or friends of friends, excessive wall posting, etc. The Team also responds to specific user complaints regarding the behaviour of applications and enforces a graduated response against the application and the application provider depending on the nature of the contravention of the Platform policy. We examined one complaint from a user in relation to unauthorised use of Intellectual Property by another developer which was received on 9 November and action was taken to delete the application within 2 hours. The account of the developer was disabled and all other applications which they had developed were also subjected to review. We also examined a phishing complaint received from a user who reported an application trying to retrieve their email and password. The application was immediately disabled and further action taken. It was also pointed out that in line with Facebook's real name culture that all applications (even those developed by the large games developers) must be developed by and attributable to an identifiable user on Facebook.

3.6.6 Process for Activating an App

A third party application is activated for a user when a user grants permission to an application to access their information via a permissions screen as below. The permissions screen (screenshot below) contains a link to the privacy policy of the third party application which the member is expected to read prior to granting permission to the application to access their information. It will be noted that the link to the privacy policy is smaller than the remainder of the text on the permissions screen. As well, there isn't any information to encourage the user that they should read the privacy policy before adding the app.

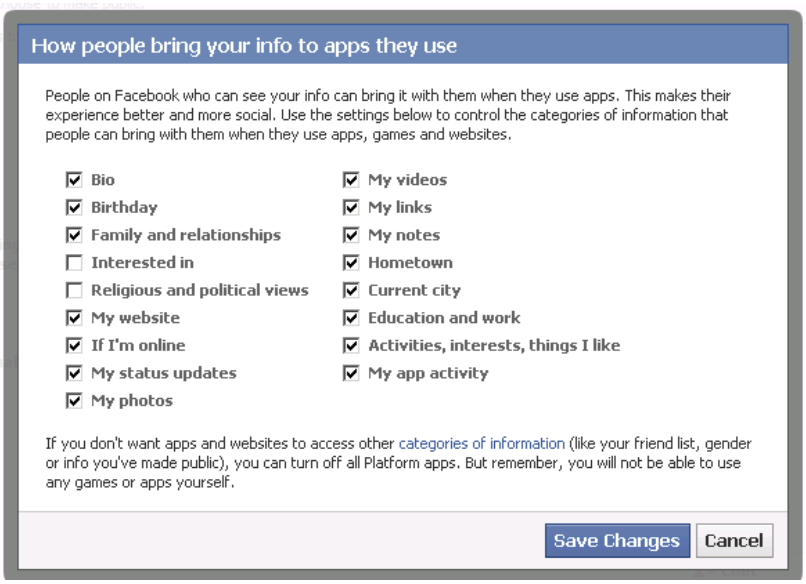




3.6.7 Consent for Third Party Applications

It is clear that users should fully understand what will happen to their data when they grant permission to an application to access their information. This is highlighted by the complaints received on this issue by the Norwegian Consumer Council and Europe-v-Facebook. This Office believes 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.

For example, when a user grants access to their information they can also grant access to information related to their friends. The extent to which the application can access information related to friends is determined by the settings of the friend. When a friend of a user adds an application, the default setting (where the user has not proactively changed their privacy settings) allows the third-party application joined by a friend to access your profile picture and name. This Office considers that the process to restrict such access is not intuitive because the user must consult the privacy settings area of the site rather than the Apps area.



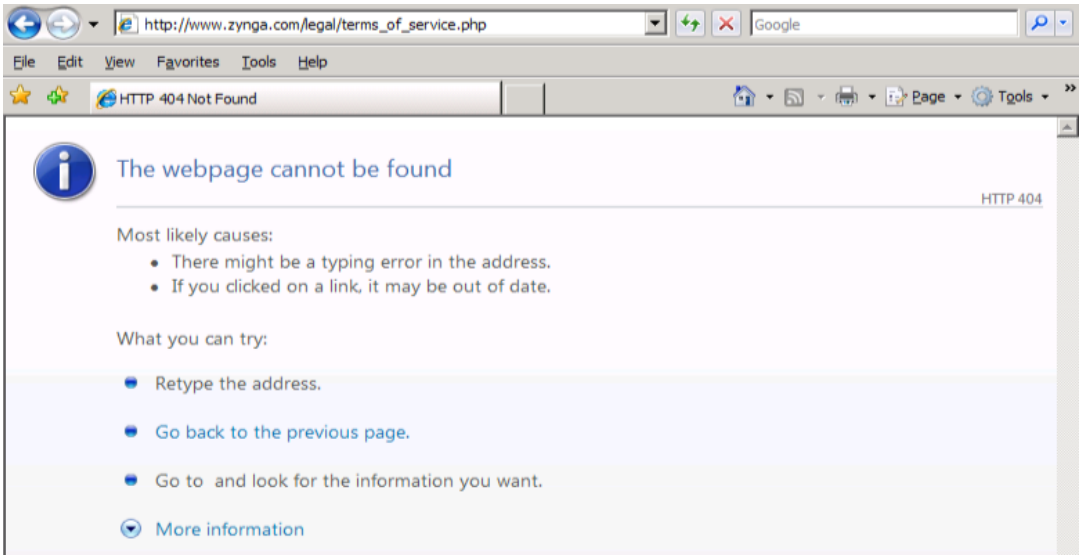
Equally when a user adds an application, the fact of adding the app is by default displayed to friends, unless the user has specifically restricted visibility using the "how you connect" privacy setting. In many cases the user's activity on the application is also displayed to friends. Again this Office considers that changing the setting is not straightforward because the user must avail of the custom settings to restrict visibility of the application to "only me". There is an additional step to set this restriction because the "only me" setting is not presented as one of the headline choice of settings such as "public" or "friends" but is contained as an option within the custom settings. From our analysis, this Office considers that many users may not fully understand that other users may see the fact that they have added an app. Additionally, the accessibility of the option to restrict visibility of their activity on the app via changing the setting to "only me" could be improved.

FB-I indicated that it had recently changed its granular data permissions dialog box (this is the information resource attached to apps which the user clicks in order to add the app). FB-I, expects

it to be fully available on all applications in February 2012 and for it to allow for contextual control over the audience that will see the user's activity. Users can also learn more about the application before adding it. In addition, applications must now use a second permissions screen for many categories of data, thereby discouraging developers from asking for too much data from users. As there is a direct correlation between the number of screens and information sought and the number of members which join an application, it is considered that this change will encourage app developers to exercise more discretion over personal data sought. This Office did note that this correlation is spelled out to app developers on the relevant screens within Facebook Platform.

As suggested earlier in this section, we would also consider it appropriate that the Privacy Policy link be given more prominence within this screen and that members 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. This would allow Platform Operations to examine the application and take appropriate action against it if it is seeking more personal data than can be justified. FB-I in response has stated that the new permissions dialog box, as referenced above, contains a "report app" link within it and that it will continue to work with this Office with the shared objective of ensuring that members have sufficient information about the use of data by the third party when making a decision as to whether to add an app or not.

Some additional issues arose while this Office was examining the role of third party applications prior to the audit. Specifically for a period of time around the end of September/start of October of this year the privacy policy link in relation to all Zynga applications was leading to a dead link as per the screen shot attached. It is assumed that this was related to an update made to its privacy policy by Zynga at that time but as the permission given by a member is entirely predicated on their ability to examine the relevant privacy policy and make an informed choice this is obviously an unacceptable situation. It is straightforward for FB-I to deploy a tool that at its most basic level will check whether privacy policy links are live. We would expect FB-I to introduce such a tool to ensure that this issue is resolved. FB-I in response has stated that it is urgently examining how to introduce this feature from a technical feasibility perspective. FB-I's progress in implementing this recommendation will be explicitly examined on our review visit in July 2012.



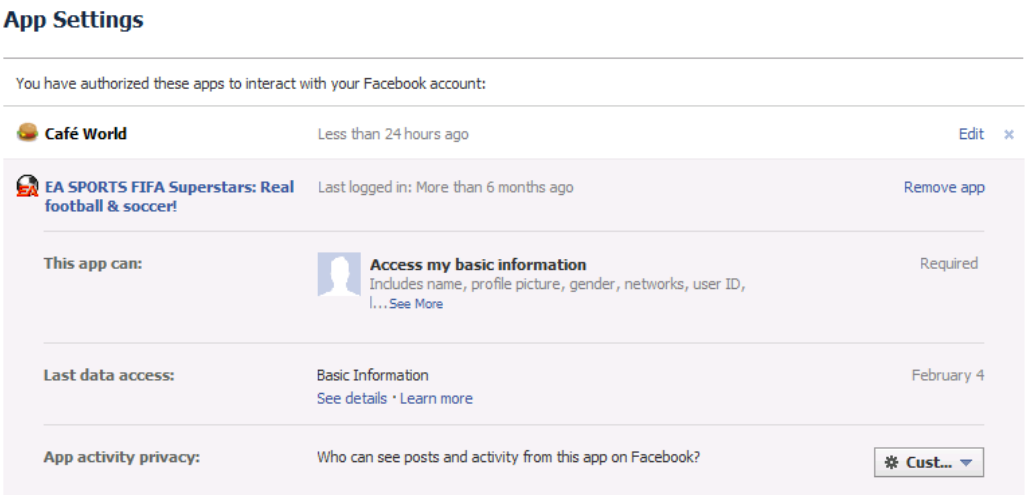
Finally in this area it was noted during the audit that Facebook has recently launched Facebook Platform for Mobile which provides a means for developers to develop mobile specific applications. A detailed examination of this Platform was outside the scope of the audit at this time given the large number of issues which were in scope. It is recognised though that there is a justifiable concern around the ability of mobile applications to collect additional information in relation to members once they have signed-up to a mobile app. While this type of information, e.g. location information, unique handset identifier as examples are not within the direct control of FB-I, there is an opportunity for FB-I to demonstrate leadership in this area and provide specific instructions to mobile applications to only seek such information where entirely justifiable and to only use it with the individual's full consent. This Office is pleased that FB-I has undertaken to bring forward appropriate guidance in this area for mobile app developers and to include relevant terms in its Platform policy.

We will examine Facebook Platform for Mobile in more detail during our follow-up with FB-I in July 2012.

3.6.8 Security Considerations

As outlined at the outset of this section, we sought to verify 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. The audit verified that this is the case. The detailed security testing undertaken to verify this issue is outlined in Section 5 - Application Development - of the Technical Analysis Report (Appendix 1).

When a user authorises an application to access their information following the procedures outlined above, the application is provided with an authorisation token. This token is then provided to Facebook along with subsequent requests for information. A user can revoke the permission for an application via the applications permissions screen shown in the screenshot below. We have confirmed that an application that has been removed by a user can no longer access their information other than that which is publicly available.



The technical analysis report also confirms that it does not appear possible for an app to perform tasks or access information unless the user has granted an appropriate permission. It is also confirmed that when a friend of a user installing an app has chosen to restrict what such apps can

access about them that this cannot be over-ridden by the app. As outlined above this Office is of the view that it is possible to make it easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way 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.

Given that the authorisation token is the means by which Facebook controls access to a user's information, we sought to examine whether the token 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. This analysis is outlined in detail in Section 5.7 of the Technical Analysis Report. We would accept that such a use of the token would breach the terms of Facebook Platform use and if identified by Facebook would lead to the taking of steps against the application by Platform Operations up to and including the taking of legal action against the app developer. We have confirmed that this is possible and also confirmed that the token also appears to remain valid when used outside the context of the Facebook Platform. This issue does pose a risk to user information in certain limited situations which FB-I acknowledges. However, as outlined in the Technical Analysis Report, the solution in place at present was introduced to deal with another security issue principally. Having considered this matter, this Office recommends that FB-I assess this matter in more detail with a view to bringing forward a solution that addresses the concerns. In the meantime, at a minimum we expect FB-I to advise application developers of their own responsibility to take appropriate steps to ensure the security of the authorisation tokens provided by it.

A number of additional examples are also outlined in Section 5 of the Technical Analysis Report which indicate that in certain cases reliance is placed on developer adherence to best practice or stated policy to ensure security of user data. This is not considered sufficient by this Office to assure users of the security of their data once they have third party apps enabled. We expect FB-I to take additional steps to prevent applications on a pro-active basis from accessing user information other than where the user has granted an appropriate permission. We will review progress on this issue when we return in July 2012.

FB-I Response

FB-I noted that Facebook is a social platform and that applications were designed to be used in a social context, largely by allowing users to interact with their friends through the app. FB-I further noted that this social dimension is a distinctive feature of Facebook apps and the primary reason why users choose to use Facebook apps as opposed to other app platforms. While it emphasises that it is the user that gives their consent for the supply of their data to the application it is committed to working with this Office to further improve the accessibility and relevance of information and controls available to users when making such decisions.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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	FB-I has recently changed its granular data permissions dialog box for apps, which was expected to be fully available on all applications in February 2012, to allow for contextual control over the audience that will see the user's activity on Facebook.	End-February 2012 and assessed again in July 2012
	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	FB-I has recently changed its granular data permissions dialog box for apps where users can choose the audience ("audience selector") for their app activity directly in the dialog box.	Assessed again in July 2012
	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.	There is a "report app" link in every dialog box, which permits users to notify FB-I of any issues regarding the app, including a missing or non-working privacy policy link. In addition, FB-I will further educate users on the importance of reading app privacy policies	End February 2012 and ongoing

		and is positively disposed to increasing the size of the link in the dialog box and will report back to this Office.	
	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.	FB-I will implement this recommendation and is urgently examining how to introduce this feature from a technical feasibility perspective.	FB-I's progress in implementing this recommendation will be explicitly examined on our review visit in July 2012.
	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 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 will positively examine alternative placements for the app privacy controls so that users have more control over these settings	FB-I will report back on this point to this Office in advance of July 2012.

	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.	FB-I will provide more messaging to developers highlighting its policy regarding sharing of authorization tokens. In addition, FB-I will commit to investigate technical solutions to reduce risk of abuse.	End of January 2012 in relation to notification to apps developers. Immediate assessment of issue identified with outcome/solution presented by end of Q1.

	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 proactive auditing and automated tools designed not just to detect abuse by developers, but to prevent it in the first place and the findings of the audit will be used to further refine the tools.	Progress review in July 2012.

3.7. Disclosures to Third Parties

A standard feature of audits conducted by this Office involve an examination of the procedures in place for handling requests from third parties to access personal data held by the audited entity. Many organisations are subject to a large number of statutory requirements which require disclosure of personal data to regulatory and law enforcement authorities upon request. The circumstances under which personal data may be disclosed to a third party are specified in Section 8 of the Data Protection Acts.

FB-I receives a large number of requests from law enforcement authorities throughout the Europe and Middle Eastern Region (EMEA). It was therefore necessary to examine its approach to the handling of these requests throughout the audit. A detailed interview was held with the Facebook Law Enforcement Team based in Dublin and subsequently with the Facebook Chief Security Officer. At the outset it can be recognised that Facebook and FB-I sit in an almost unique position given the vast number of users and the justified and specific concern to ensure that Facebook is a safe place for minors aged over 13 to interact with their friends. There are well-documented cases where internet platforms, including Facebook, have been used by individuals for criminal and other inappropriate purposes. FB-I indicates that it places a high priority on addressing such behaviour and as a consequence has a large focus on identifying and dealing with any such activity. This consequently requires it to have an ongoing and constructive relationship with law enforcement authorities around the world. As part of its overall safety efforts, FB-I has indicated that it dedicates substantial resources to identify and promptly address any instances in which users seek to use the site to exploit children, perpetrate frauds, or otherwise facilitate illegal activity.

The staff in the FB-I law enforcement unit have all undergone extensive training in the handling of personal data. Staff members with decision making authority to provide data must additionally have achieved a recognised certification in privacy.

The focus of the audit in this area was to establish that FB-I had fully assessed the legal basis in Irish law under which it could comply with requests from law enforcement agencies. FB-I in response to a request from this Office have provided a detailed and comprehensive assessment which is at appendix 5.

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 order to assess whether FB-I was appropriately applying this criteria, five random recent requests received from law enforcement authorities were examined. These requests were received from the UK, Italy, Belgium, Germany and Ireland. In all cases, the requests received cited a relevant legal basis underpinning the request and in the case of the UK, all such requests are now coming from designated single points of contact (SPOC). The advantage of this approach is that it minimises the risk of inappropriate requests for data as all such requests must be gated

through designated expert staff in each UK Police force. It was clarified that the legal basis cited in each request is examined for compatibility with applicable law and if any doubt arises further advice is sought from in-house or external legal counsel. Two of the cases related to missing children and therefore regardless of the legal basis that was cited FB-I could also have relied upon Section 8(e) of the Acts which allows for disclosure, inter alia, where the life of a person may be at risk. It was also confirmed that all requests are either made to a dedicated fax machine or via email with all responses issuing by encrypted email.

FB-I has emphasised that it does not respond to law enforcement requests which are broad in nature or seek data on more than one user. One of the sample law enforcement requests examined was refused on this basis. FB-I has emphasised that *"should the law enforcement agency require content information from FB-I, we will require that we be served with a legally compelling request under Irish law. The Gardaí (Irish Police) will be required to produce a search warrant or similar coercive document. Non-Irish search warrants will only be respected by FB-I if they are enforceable as a matter of Irish law. This will require that any such orders be domesticated by way of application to the Department of Justice pursuant to the Criminal Justice (Mutual Assistance) Act 2008."* The non-provision of content data was confirmed by examination of the sample requests examined.

3.7.1 Analysis

As outlined above, Facebook by the very nature of its service will continue to receive law enforcement requests for access to information. FB-I 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.

This Office recommends a continuation and extension of the SPOC arrangement with law enforcement authorities. As the requests are made to FB-I it is important that any such forms etc developed for this purpose make clear that the responsible entity is FB-I. At present any requests for user data under the control of FB-I are returned if they are not correctly addressed. 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. It is not a sufficient safeguard for the requests to issue from a designated email box as such a box can be used by multiple users. We also recommended 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. 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.

FB-I in response has indicated that it is implementing the above actions.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I is implementing these recommendations.	To be commenced by Facebook in January 2012 and reviewed in July 2012.

3.8. Facial Recognition/Tag Suggest

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. Facebook indicates in its data use policy that these suggestions are made by saving certain information about the photos people are tagged in and comparing that information to newly uploaded photos to see if the newly uploaded photos are similar.

If Facebook cannot suggest a name automatically, it groups similar photos together so the user can label them quickly and let friends know that a user has posted photos of them.

The operation of the facial recognition/tag suggest feature was the subject of previous communication by this Office with FB-I following public concern on foot of its launch in the EEA. It was also examined and remains under examination by other data protection authorities. Our communication with FB-I at the time was not on foot of a complaint and sought to progress the matter to a satisfactory outcome that would be acceptable to all parties. The outcome agreed was not taken in the context of a formal decision of the Commissioner. At that time FB-I, while pointing to the information that was in its original Privacy Policy, along with further information given via its blog, a specific change in its Data Use Policy announced in December 2010, and the possibility to disable the auto-tagging feature via the user privacy settings, agreed voluntarily to take additional measures for users in the EU:

- Each user was given prominent notice of the new feature on her/his Facebook 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.

The operation of this tag suggest feature was also the subject of **Complaint 9 – Face Recognition from Europe-v-Facebook.** The complainant contended that Facebook's photo-tagging suggestion feature involves the analysis of tagged photographs held within its systems. The complainant quoted Facebook's Privacy Policy which states that *"if one of your friends uploads a picture of you, we may suggest that your friend tag you in the picture. We do this by comparing your friend's pictures to information we've put together from the photos you've been tagged in."*

The complainant has highlighted a number of issues of concern in relation to this feature. Firstly, he contended that Facebook is not admitting to the generation of biometric data. Secondly, as the feature is relatively new, users already signed up to Facebook might not have agreed to the new feature and have not been asked by Facebook to agree to the new features in the Privacy Policy. Thirdly, he contended that users were not provided with any specific information on the introduction of the feature. Finally, he stated that the feature is very difficult to de-activate and

that even when a user has successfully deactivated the feature, any generated biometric data remains.

Facebook indicated in response that it does get the consent of users, pointing to the fact that users do not have to participate in the tag suggestion feature and may disable it at any time. Facebook also pointed to the revised wording in its Privacy Policy which 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.*

In relation to deleting the feature, Facebook stated that instructions on how to do this are made clear in its Help Centre which states that

> *disabling tag suggestions will result in the deletion of the photo-comparison data that we use to make Tag Suggestions work.*

thus implying, stated Facebook, that there is no further processing of this data after deactivation.

FB-I also wished to clarify in precise terms how the "Tag Suggest" feature operates. Facial recognition software is an algorithm that is applied to review the image of a face and calculate a unique identifier, which is a string of numbers ("number"), based on distinguishing characteristics, such as the shape of the eyes and the distance between eyes, nose, and ears. Once the number is calculated, a new image can be evaluated by the algorithm, converted to a number, and compared with a previous calculation. If the numbers are the same, a match has been identified.

There are several important details about the way Facebook's Tag Suggest feature works which FB-I wished to emphasize:

1. It requires only a few tagged photos of a user in order for its facial recognition algorithm to calculate the number;
2. The number is constantly being updated based upon newly tagged photos;
3. Facebook's facial recognition technology is not structured to be able to take a random photo and match it to a photo in its databases, but rather is structured to be able to suggest specific friends to a user;
4. Photo-tagging using the tag suggest feature is not automatic but rather the user has to approve the tagging of the suggested friend;
5. A Facebook user is suggested only the names of friends from his or her closest circle of friends to tag in an uploaded photo, if there is a number match;
6. Given a number you can NOT recreate the image or do anything besides match it to another number; and
7. The number is only of a single face, which means you can have multiple numbers in a single photo (assuming there are multiple faces).

3.8.1 Analysis

At the time of this Office's previous communications with FB-I on this issue we made clear our strong preference that the measures subsequently taken should have been in place before the auto-tagging feature was launched for EU users.

Subsequent to that interaction with FB-I, the Hamburg data protection authority has separately considered this matter and has reached a conclusion in line with the provisions of German data protection law.

This Office in the context of the current complaint has re-examined this matter. It remains our position that FB-I should have handled the implementation of this feature in the EEA in a more appropriate manner. The creation of the facial recognition identifier does constitute the processing of personal data and we do consider the creation of the identifier to constitute biometric data in relation to the user. Biometric data are not among the data categories given special protection in the Irish Data Protection Acts or in the EU Data Protection Directive. Our consideration of this issue must also have regard to case law[23] in Ireland regarding the use of biometrics. This case law has not considered that the processing of biometric data requires explicit consent. On the other hand, biometric data have been afforded special protection in the laws of certain States, and the EU's Article 29 Working Party has suggested that such a categorisation should be considered in the future EU data protection regime[24]. We therefore recommend from a best practice perspective that FB-I take additional action.

We also took the opportunity on the audit to examine the code path executed when a user disables the "tag suggest" feature to ensure that the data representing a user's facial profile is appropriately deleted if the user decides to disable this feature. We have confirmed that the function used to delete the user's facial profile is invoked when the user disables "tag suggestions".

FB-I's Response

FB-I indicated from the outset its strong belief that it had obtained consent from users through their agreement to its Data Use Policy when they join Facebook to do the minimal additional processing of their photographs to make this popular feature possible. It stressed its belief that the processing is minimal because the use of the feature only offers a technical convenience and does not permit anyone to identify or tag someone who is not already their friend – the only people who can benefit from the *"Tag Suggest"* feature and the related processing are a user's friends, who could presumably have been able to recognize and tag the user themselves.

In consultation with the Commissioner, we provided additional notice to EEA users, including a direct link to disable the feature, by running the equivalent of advertisements on their home pages. We maintain that we have complied with Irish and EU Data Protection law, and are not obliged to do anything further. However, in the spirit of continuing cooperation, 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 they interact with it by selecting either option presented then it will disappear for the

[23] Dunnes Stores vs Data Protection Commissioner, Circuit Court Appeal of an Enforcement Notice April 2010
[24] Advice paper on special categories of data ("sensitive data") (20 April 2011)

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 the Learn More link and will also be shown if a user clicks Adjust Your Settings.

3.8.2 Analysis

For the reasons outlined above further notification in relation to the current deployment of the feature is not strictly legally necessary under Irish law. This Office therefore welcomes the commitment of FB-I to adopt a best practice approach in this area. We would further expect that FB-I take a similar best practice approach and allow users to opt in to any further expansion of the Tag Suggest feature that would allow suggestions beyond just Friends.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	First week January 2012 at the latest

3.9. Data Security

3.9.1 Introduction

Organisations are required by data protection law to hold personal data securely and to only make personal data accessible to third parties with the consent of individuals. In the case of Facebook individual users are not, in general, in a position to conduct an assessment of security and rely therefore on affirmations made by Facebook in this respect.

An assessment of security policies and practices including access control within an organisation is a standard feature of all audits conducted by this Office. Clearly the size and scale of Facebook increases both the security risk to be assessed and the nature of the assessment. As outlined in the introduction to this report the constantly evolving nature of Facebook is a challenge in and of itself in trying to identify data protection and particularly security risk. Indeed as one of the world's most prominent online services, Facebook is a particular target for attack. Individual users also are a target for attack and Facebook estimates that there are in the region of 600,000 attempts per day to hack into or gain control of user accounts. This requirement to protect its systems and its users does, as outlined in the Retention section of this report, create a tension between the data protection requirement to only collect and hold the minimum amount of information necessary for a specific purpose and the data protection requirement to protect personal data from inappropriate access or disclosure. A potential resolution of that tension is suggested in the Retention Section of the Report. Security issues around third party applications are separately assessed in that section of the report.

This Section therefore focuses on the security policies and practices within Facebook to protect user data from inappropriate access. To assist this Office in conducting this assessment, a member of staff of the UCD Centre for Cybersecurity & Cybercrime Investigation which is part of the UCD School of Computer Science and Informatics was provided to this Office for the conduct of the audit. The staff member was appointed as an authorised officer of the Data Protection Commissioner and therefore enjoyed all the same rights of access to data held by FB-I as the other members of the audit team. The detailed security and Technical Analysis Report produced further to the priority issues identified by this Office is attached at Appendix 1. As indicated above, the constantly evolving nature of Facebook and indeed the security threats on the internet mean that the report can only be considered a reliable assessment as of the date of its completion. This is an area which will need to be kept under constant scrutiny by this Office and will certainly be revisited in July 2012.

Data security was also a focus of the complaints received on this issue. **Complaint 12 – Data Security** from **Europe-v-Facebook** sets out a number of security concerns in relation to how Facebook holds personal data. In relation to encryption, the complainant contended that it is only applied to password and credit card information and not to other forms of personal data held. In terms of Facebook's Privacy Policy, the complainant considered that Facebook does not take enough responsibility for data security in its privacy statements, for example:

> *We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available.*

And

We do our best to keep Facebook safe, but we cannot guarantee it.

The complainant also wished to highlight what he considers to be a lack of control over data being provided to third party applications, some of which may fall outside the Safe Harbor agreement, and a lack of enforcement by Facebook in terms of the provision of a privacy policy by third party applications. This aspect is addressed in the third party applications section.

FB-I considers that its data security provisions meet and exceed industry standards. Facebook stated that it provides additional security features to users through their *'security settings'* which allows, for example, users to have all their communications with Facebook via https where available if they prefer.

In terms of its privacy statements, FB-I commented that its *"contractual commitments to user security need to be carefully circumscribed and candid so users appreciate the security risks which exist and which can never be fully eliminated."*

Regarding the issue of third party applications, Facebook stated that complainant's allegations are unfounded. A more detailed response on this issue is provided in Complaint 16.

3.9.2 Complaint 19 – Pictures Privacy Settings indicated that Facebook allows users to upload photographs to their Facebook page and are given the option to apply their own security settings. The complainant stated that Facebook has outsourced the delivery of the picture content to a company (Akamai Technologies) and, by using the source code from the pictures page of Facebook.com and identifying certain URLs, that it is possible to view some photos that should be hidden from view.

3.9.3 Complaint 20 – Deleted Pictures relates to the previous complaint. It outlines that users are given the option to delete pictures they have uploaded to Facebook. Again, by using the source code from the pictures page of Facebook.com and identifying certain URLs, the complainant stated that it was possible to view a photograph for up to 48 hours after he had deleted it from Facebook.

Facebook stated that it deletes photographs *"as quickly as technologically feasible"* and commented that once a photograph is deleted, it is then unavailable on Facebook.

Facebook indicated that users are informed of possible delays in deleting data in its Statement of Rights and Responsibilities.

This issue is covered in more detail in section 7.4 of Appendix 1.

3.9.4 Analysis

It was therefore incumbent upon this Office to devote a significant focus during the audit to assessing security issues. A dedicated security team therefore worked through security related matters with FB-I throughout the on-site element of the audit and afterwards. Facebook provided its most senior engineering personnel in this area to our Office and made such individuals

available on an ongoing basis following the on-site element as more detailed assessments were carried out on discrete items as outlined in the Technical Analysis Report.

It is important to state at the outset that as could be expected FB-I places an enormous and ongoing focus on the protection and security of user data. Our audit has confirmed this focus.

3.9.5 Protection of User Data

Facebook has provided a number of tools to users to enhance their security while they use the site at a desktop or via a mobile device. These tools which are available to users via Account Settings – Security are assessed in the Technical Analysis Report. We would consider that they do provide a more than reasonable framework for the user who wishes to have in place additional security protection while using the site. Over and above these optional features FB-I as detailed in the Retention section collects extensive information of the log-in activity of users principally via cookies. The technical details of the cookies utilised by Facebook in a range of scenarios are outlined in Section 6 of the Technical Analysis Report. FB-I makes innovative use of these cookies to identify unusual or suspicious activity on an account. The use of this information to detect, identify and prevent malicious activity on user accounts was demonstrated via sessions with the security, risk & platform operations and user operations teams. This Office is satisfied that FB-I is very pro-active in this area. In fact the only issue that has arisen is that thus far perhaps from a data collection and usage perspective it has adopted an over-zealous approach.

3.9.6 Information Security Assessment

Facebook does not have an extensive written information security policy. It has preferred instead to focus on the achievement of high level principles. Several particular areas pertaining to corporate information security were discussed with Facebook. The following items in particular were noted:

- Facebook perform constant penetration testing on their entire external IP address range.
- Facebook perform constant penetration testing on their internal networks.
- All employees, contractors and vendors are subject to the information security policy, and are required to familiarise themselves with the terms of the policy on a regular basis.
- Regular, company-wide security awareness training is carried out.
- Employees, contractors and vendors are required to sign a non-disclosure agreement before access to user data is granted.
- Contracts with third parties contain security and privacy requirements and periodic reviews of third party compliance with these requirements are carried out.
- A due diligence process exists that is used to assess if a third party has the capability to comply with the security and privacy requirements.
- An identity management system has been deployed to provision accounts, remove accounts and manage access rights.
- All users are assigned a unique user name and password. Password policy requirements are enforced on all systems.
- Credentials required to access production systems automatically expire on a regular basis requiring a manual process to re-enable access.
- A manual process is required to grant an employee access to Facebook user data. The process requires approval by the data or system owner.

- Currently access rights are tool based, meaning that an employee with access to a particular tool can access any user data accessible through that tool. A new, software token-based access management system is under development to enable more fine-grained access control to user information.
- A valid certificate of PCI DSS[25] compliance pertaining to the storage of customer financial data has been presented.

An assessment was carried out of the current access levels of employees within FB-I to user data. We also noted the user access policies, employee contract, frequent staff notices and training materials made available to employees warning of the fundamental need for confidentiality in relation to user information. We also received an overview of the audits undertaken of staff access to user data in response to concerns and on a random basis. FB-I indicated that when an employee accesses user data, extensive logging information is collected and processed on a daily basis, highlighting any instances where abuse is suspected. The logs are also used for forensic investigations when there has been a complaint of inappropriate use. Investigations look at when user information was accessed by the employee and what type of data was accessed to ensure it is consistent with the request the employee was fulfilling. We are satisfied following that assessment that FB-I does at present have in place an appropriate framework to ensure that all access to user data is on a need to know basis. We did however encourage FB-I to expand its monitoring to ensure that there was no employee abuse through an inappropriate password reset of a user's account that would enable the employee to regain access. FB-I has undertaken to integrate user password resets by employees into its monitoring tools.

However, we were somewhat concerned that the provisioning 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 to see. In this respect FB-I provided a detailed outline of the new access provisioning tool it is developing that will allow for more fine-grained access to user data. It indicated that access provisioning will be granted based on the employees department, physical location, and specific job duty they perform, which will be driven from the HR system. This new provisioning process will ensure employee role changes result in the necessary permissions changes as well. This is to be welcomed but given the requirements in this area, this Office will thoroughly review the application and usage of the new token based tool in July 2012.

The majority of the controls described by FB-I appeared to this Office to be effective. It can be reasonably concluded that if large-scale, frequent data breaches were taking place on Facebook's corporate networks, that this would be widely reported, particularly considering Facebook's global profile. Since this is not the case, the information security controls in Facebook appear to be preventing these types of incidents.

From a standard assessment perspective, if there is a shortcoming in Facebook's information security arrangements it is their informality. Many policies and procedures that are in operation are not formally documented. FB-I will continue to document policies and procedures as required to maintain consistency in security practices.

[25] Payment Card Industry Data Security Standard. See https://www.pcisecuritystandards.org/security_standards/

3.9.7 Security of Pictures Uploaded to Akamai

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 store copies of content on servers geographically closer to the users of that content than the source servers. At present Facebook's data centres are located only 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. The services of Akamai are used by a large number of websites for this purpose.

The security assessment of this issue is outlined in detail in Section 7 of the Technical Analysis Report (appendix 1). The issue to be assessed was whether it was even remotely possible for a person who would not otherwise have access to an image uploaded to Facebook to obtain access to that image or indeed any image on Facebook to which they did not have access rights. This Office is fully satisfied that the randomness of the url string generated for each image is such that there is no realistic possibility of such access taking place unless, of course, a user with access to the image provides the url string of the particular image to a third party. Equally if a user already has legitimate access to an image and therefore the url string, cutting and pasting that string into a browser and accessing the image outside of Facebook does not give rise to any additional concern. Therefore the conclusion reached is that 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. *FB-I notes that this issue was a topic of the FTC's proposed complaint and settlement agreement noted above.*

We are aware of a bug, reported in early December 2011, that allowed unauthorised access to photographs in narrow circumstances, but this matter was unrelated to the basis of the complaint or our assessment and has been resolved.

3.9.8 Deletion of Facebook Photo

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

The original image URL will continue to return the deleted photo for a period of time. FB-I indicate that the Akamai cache retains content for on average 14 days but no more than 30, after which point it is removed from the cache. As above, in order for a third party to retrieve from the Akamai cache a picture that a user has deleted from their Facebook profile, the attacker must therefore have prior knowledge of the photo URL. In such cases, to retrieve the photo URL from Facebook, the attacker will most likely have viewed the image from the user's profile in their browser. Therefore, they may also have copies of the image cached locally on their PC and/or transparently cached, for example, by their Internet service provider.

FB-I is reviewing the period of time that images are cached in the Akamai cache but for the reasons outlined above this Office does not consider that any specific security issue arises for which any amendment in current practice is required.

3.9.9 Screen 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 such an automated process to gather a large volume of information about Facebook users through a scraping technique. FB-I have provided details of the arrangements that they have made to prevent scraping to this Office.

We believe that the current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data while allowing the service to be effectively provided to legitimate users.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
Security	Many policies and procedures that are in operation are not formally documented. This should be remedied.	FB-I will continue to document policies and procedures as required to maintain consistency in security practices.	Newly documented policies and procedures to be reviewed in July 2012.
	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 will integrate user password resets by employees into our monitoring tools	End-January 2012
	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 is implementing a new access provisioning tool that will allow for more fine-grained control of access to user data.	We will thoroughly review the application and usage of the new token based tool in July 2012.

	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		
	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.		

3.10. Deletion of Accounts

The Data Protection Acts provide a right for an individual to seek deletion of information held by a data controller in relation to them except where a data controller can justify such retention, e.g., by demonstrating that the organisation can rely on "legitimate interests" to retain data. Complying with requests from members for deletion of their accounts has reportedly proven difficult in practice for Facebook it was assumed due to the complexity of its system.

While the theme of retention and deletion of specific items of information is dealt with elsewhere in this report, a detailed focus was placed on the procedures and protocols in place in FB-I to comprehensively comply with account deletion requests from members in a timely manner. We therefore met with relevant team members from Facebook and received a detailed system architecture overview in order to better understand any complexities in the deletion process. This focus arose from a pre-audit concern that a 90-day period for the deletion of personal information following a request from a user was overly lengthy.

By way of background, Facebook users can choose to either deactivate or delete their account[26]. If a user chooses to deactivate their account, this means that the user's profile information will no longer be available on Facebook, effective immediately. However, Facebook currently retains the user's information indefinitely in case the user chooses to reactivate their account at some point in the future. The retention aspects of this are dealt with in that Section of the Report.

A request by a user for the deletion of their account, on the other hand, is meant to lead to the permanent removal of the user account from Facebook. The process followed when the user requests that their account is deleted is described here and in more detail in the Technical Analysis report at Appendix 1.

3.10.1 Deletion Process

FB-I informed this Office that after a user submits a request to delete their account, their account enters a state of "pending deletion" for a period of 14 days. During this period it is possible for a user to change their mind and cancel the deletion request. FB-I stated that this 14 day period is provided for various reasons, including allowing the user a "cooling off" period and also for the case where someone with unauthorised access to a user account issues a delete instruction. FB-I indicated that some 40% of account deletion requests are altered within this 14 day period.

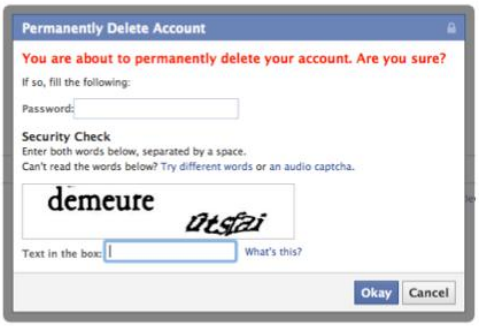
If the user logs back in to their account during the 14 day period where the account is pending deletion, they are presented with a message stating *"Your account is scheduled for deletion. Are you sure you wish to permanently delete your account?"* The user can then either confirm or cancel the deletion request. Once the 14 day period has expired, an account deletion framework is activated which deletes account information. It is not possible for the user to log-in after this time.

Below are some screenshots of the process.

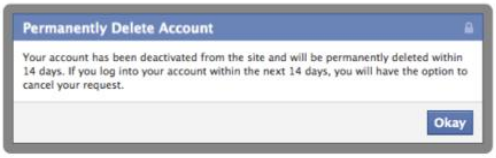
[26] http://www.facebook.com/help/search/?q=how+do+i+delete+my+account

1) https://www.facebook.com/help/contact.php?show_form=delete_account

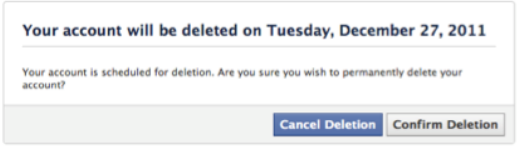
2) Password and Captcha



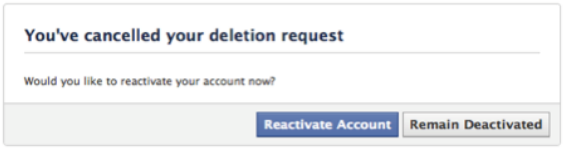
3) Confirmation and information



4) If the user logs into Facebook (or attempts to use Connect or mobile applications) they are presented with the choice of canceling the pending deletion or not logging in



5) Cancel Deletion: User is presented with the choice of reactivating the account remaining deactivated



3.10.2 Deletion Verification Tests

In order to assess the effectiveness of the deletion process deployed by Facebook two tests to verify the status of a deleted account were performed during the on-site element of the audit.

FB-I was provided with the email address and full name of a user who had requested that their account be deleted on 2 August 2011. This individual had brought this account deletion request to the attention of the Office in advance of the audit and had sought confirmation that their request was in fact carried out. The email address and the full name of the former user were only provided to FB-I immediately in advance of the test. FB-I was asked to provide any information that was available on their systems relating to this email address or full name. This test was performed under supervision by our technical team and notes were made of the activities performed.

In the event no details relating to either the email address or full name were found. The process used to search for the email address and full name were repeated with known Facebook user email addresses and full names to verify that if the account under test still existed, the searching performed by Facebook would have revealed the account information. This was verified as returns were noted in relation to the known details.

FB-I were provided also with an IP address and asked to produce any information relating to browsing activity originating from that IP address. Facebook had no prior knowledge of the IP address.

Originally it was expected that the search would be performed over a 90-day period, however the Facebook log querying interface can in principle, but cannot in practice, query such a large date range. For illustrative purposes, querying Facebook's logs to identify the activity associated with a particular IP address in any given 24 hours period takes approximately one hour. The period of the search was therefore reduced to five days.

No browsing activity was identified as being associated with the provided IP address. FB-I acknowledged that this was an unexpected result for any IP address that is being used actively for browsing. No additional information is known about the browsing patterns associated with the IP address, however there are a number of possible explanations for this result which are outlined in the Technical Analysis Report.

A further demonstration was performed to show that after an account has been deleted, no information about that account (except for the fact that the account used to exist and has now been deleted) is visible via a userid in internal Facebook tools.

3.10.3 Account Deletion Framework

FB-I during the detailed examination of this issue adopted an open and transparent approach with this Office in relation to their current account deletion processes. In particular,

- There has been an inability to reliably verify that a user's account information has been fully deleted.

- If, for any technical reason, the deletion process failed or crashed, there was no way to retroactively seek out and delete information that was no longer associated with any active account.

Facebook started working in 2010 on putting into production a new deletion framework that is seeking to address these issues and thereby reliably delete user accounts. The framework is well developed with regard to deletion of user-generated content, and ongoing related to deletion of logs. In this respect, a due diligence process was conducted to exhaustively identify all locations where user data is stored and to ensure that

- All new account deletion requests delete all user data from all possible locations.
- The new account deletion framework is applied to all previously processed account deletion requests that may not have adequately purged user data from all possible locations.

We reviewed the new deletion process as outlined in Appendix 1. In summary, the data associated with an account can be roughly split into online data directly used to serve web pages to users, and log data. Online data for deleted accounts was reviewed and in all cases examined, no remaining data was found. Some data can remain after deletion, as described in Section 10.3 of Appendix 1.

Samples of log data were reviewed in their original form and the rewritten form after the user ID has been replaced with a random ID and other identifying information has been removed, as described in Section 10.3.2 of Appendix 1. We confirmed that the new log rewriting functionality operates as intended.

Data that cannot easily be located as it was only linked indirectly to the user is proving problematic to delete, but work is underway to address this issue through the new framework.

3.10.4 Shared Content

FB-I also confirmed that it faces a particular challenge in meeting account deletion requests in relation to shared objects such as groups, pages and events. This is understandable as it would be inappropriate to meet with one user's request for account deletion by deleting content which might be considered also the personal data of another user. A number of scenarios are outlined in the Technical Analysis Report.

At the present moment, while most shared content is deleted when one party deletes it, some shared content either: 1) in the case of Messages, is not deleted until all parties have deleted the content, and 2) in the case of some Groups content such as posts made by a user are not deleted. FB-I reports that it is working to delete such Groups content and that the difficulty lies in the fact that it is a category of data that is computationally difficult to find to delete.

This is because there is only a one-way relationship stored in Facebook's data relating the group post to user ID. This relationship allows the user's profile picture to be looked up and displayed beside the content of their group post.

A solution is currently being implemented to convert this one-way relationship into a two-way relationship, allowing all of the user's group posts to be efficiently identified and removed when the account is being deleted.

3.10.5 Analysis

There is a requirement for FB-I to have a robust framework in place to delete user accounts following a request. The decision by Facebook to apply an initial 14-day moratorium on the request in case the user changes their mind is not challenged based on the figures provided by FB-I of the number of individuals that change their decision.

At the time of the conduct of the audit it was clear that Facebook would have preferred for a more robust account deletion process to be fully in place for verification by the Office. However, we returned on 14 December and were in a position to note a substantial improvement in the process following the conduct of testing as outlined in the Technical Analysis Report. However, it is estimated by FB-I that it will be six months before the log re-writing functionality is fully rolled-out and deployed to all previous account requests to ensure that all data is deleted. We will therefore fully review this process in our July 2012 review.

On an overall basis, it would be the view of this Office that the effective deletion of a user account should take place much quicker than 90 days and accordingly we will also be reviewing this aspect in July and in order to do so will ensure that a number of account deletion requests at varying intervals are in a position to be assessed to confirm the precise period of time that account deletion is taking. FB-I noted that the primary data associated with an account is deleted at the 14-day point. The data that remains after the 14-day point are backups that have not yet been purged (e.g., MySQL backup tapes) and log data that is in the queue to be rewritten. In this respect, this Office can acknowledge that we would not normally consider that the obligation to delete personal data on request should apply to back-up data within the required 40 day period for precisely the reason FB-I have outlined below. FB-I stated that it refers to a 90-day period to capture this backup data, which is essential to being able to recover from a problem on the site. FB-I indicated that it had already devoted a substantial amount of engineering resources to progressing account deletion to an acceptable level and was committed to working towards the objectives outlined by this Office.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.)	FB-I had already devoted a substantial amount of engineering resources to progressing account deletion to an acceptable level and is committed to working towards the objectives outlined by this Office.	Review in July 2012

3.11 Friend Finder

One of the most consistent sources of complaint and query to this Office is the operation of what is known as the friend finder feature by Facebook. The operation of the feature is described in the specific complaints below. The source of query and complaint is that the feature generates invitations to non-users of Facebook and based on uploaded contacts it can inform these non-users of multiple people on Facebook whom they may know or have had contact with. For non-users the feature can give rise to justifiable questions and suspicions as to how Facebook was able to identify their relationship to other users. In summary Facebook is able to make these connections as it maintains a record of members who have uploaded an individual email address and cross-references between the various members who have done so to make friend suggestions in invitation emails sent by users to non-users. It also engages in such cross-referencing to make suggestions to members who are not active on the site. FB-I only cross-references the email address of a non-user in this way after the non-user has received an email invitation from a user and has been given notice that Facebook has their email address and an opportunity to opt-out of such processing.

3.11.1 Complaint 2 – Shadow Profiles the complainant stated that Facebook is gathering information in relation to users and non-users of Facebook through a number of functions including the synchronisation of mobile phones, importation of personal data from email contact lists, instant messaging services and through invitations sent to friends. This information primarily consists of email addresses, but may also include names, telephone numbers and addresses. The complainant contended that the information is being used to add to Facebook's information in relation to users and to create shadow profiles of non-users of Facebook without the knowledge of the data subject. The complainant added that some of this information may be of embarrassment to the data subject.

In response to his access request to Facebook, the complainant stated that he did not receive any information in relation to other people who may have uploaded his personal data to Facebook through synchronising their mobile device or uploading their email contact list.

The complainant considered that Facebook is in breach of a number of areas of data protection legislation, including the fair processing principle and that the collection of the data is excessive. In addition, he stated that Facebook's Privacy Policy does not contain any notice to inform users that shadow profiles are held, for what purpose they are being used and that non-users have not given their consent for the retention and processing of this data.

Facebook stated that non-user data is imported when the data is uploaded to a user's Facebook account but that this information is only used to facilitate the user in sending invitations to non-users.

Facebook stated that when an invitation is sent to a non-user by a user, the non-user is clearly informed that Facebook has his or her details and offers a link to allow the non-user to delete their email details. Facebook stated that it retains a non-usable hashed version of the email details in order to prevent any further emails being issued to that address, for example, in a case where the non-user's details were subsequently uploaded by a second user.

Facebook clarified that it does not hold *"Shadow Profiles"* of non-users.

3.11.2 Complaint 4 – Synchronising

As highlighted in Complaint 2, Facebook offers a facility to allow users to synchronise their mobile phones or other devices with Facebook, thus allowing users to find people they know on Facebook. The complainant was of the view that the synchronising process involves all personal data on the device being transferred to Facebook and that if, for example, an individual does not want his work email address or telephone number to be known to Facebook, he has no option to prevent Facebook from collecting this personal data through the upload of information by a Facebook user.

The complainant stated that the user or data subject has not provided their consent for their personal data to be collected by Facebook. In addition, the complainant considered that Facebook is in breach of data protection legislation as it is processing the collected data in order to match users, send invitations and advertise Facebook services.

Facebook described synchronisation as an optional service that allows users to back up their mobile contact details. Users may subsequently choose to issue friend requests to uploaded contacts.

Facebook clarified that it does not process all personal data on the device. The only data which can be synchronised are names, phone numbers and email addresses.

As with Complaint 2, Facebook pointed to extracts from its Data Use Policy in response to the issues raised. In the section "some other things you need to know"[27], Facebook pointed out that

> *We offer tools to help you upload your friends' contact information so that you can find your friends on Facebook and invite friends who do not use Facebook to join. If you do not want us to store this information, visit this help page[28]. If you give us your password, we will delete it after you upload your friends' contact information.*
>
> *Invitations*
> *When you invite a friend to join Facebook, we send a message on your behalf using your name, and up to two reminders. We may also include names and pictures of other people your friend might know on Facebook. The invitation will also give your friend the opportunity to opt out of receiving other invitations to join Facebook. Where the friend has not opted out, we may also include names and pictures of other people your friend might know on Facebook.*

In relation to non-users having the opportunity to opt out, Facebook indicated that they offer a link to allow the non-user to delete their email details. Facebook contends that it has the implied consent of the non-user to process their information if the user decides not to instruct Facebook to remove their data. Facebook further noted that it will not contact a non-user unless it is instructed by the user who uploaded the contact information.

[27] http://www.facebook.com/full_data_use_policy#otherthings
[28] https://www.facebook.com/contact_importer/remove_uploads.php

3.11.3 Analysis

The friend finder feature (as it is called), as well as the inclusion of people a non-user may know ("people you may know") in email invitations sent by users has been previously examined closely by data protection and privacy authorities. At present the Office of the Privacy Commissioner of Canada (OPC) is concluding an investigation on both friend finder and people you may know. In order to ensure the best use of limited resources, we discussed with that Office its preliminary findings in advance of our onsite audit. Our Office concurs with the findings which the OPC intends to make in this area and therefore has not re-examined them in the context of this audit. FB-I has already implemented the same changes to these features as Facebook Inc. did during the OPC's investigation. These changes should serve to improve the ability of a non-user to clearly understand the use of their email address by FB-I and request the cessation of this processing.

One small caveat to the above is that even after an individual has opted out from further contact from Facebook they will still receive private messages sent by users of Facebook. As these messages behave like any normal email system there is no requirement to apply the opt-out to such messages and to do so would interfere with the private communications of individuals.

As there is no Facebook presence in Canada, our colleagues were not in a position to assess the actual use of the friend finder technology within Facebook and therefore we focused our efforts on such analysis. Based upon the previous analysis by the Canadian and Hamburg data protection and privacy authorities, this Office was satisfied that the upload of contacts by individuals to facilitate the sending of invitations to friends could operate in compliance with the Data Protection Acts provided full information was provided to non-users in relation to the use of their email address data on receipt of an invitation and any requests for removal are respected. We have confirmed that the email addresses of non-users who have opted-out from further contact are held in an appropriate hashed form and are not available for any further use.

3.11.4 Security of Password

The Office also took the opportunity of the audit to confirm that passwords provided by users for the upload of contact lists for friend-finding purposes are in fact held securely and destroyed. This was tested on 17 November 2011 and it was confirmed by examination of the relevant code that uploaded passwords are only stored in memory for the period necessary to access the external email account and are then discarded.

3.11.5 Technical Examination

An examination of the technical operation of the friend-finder feature and the synchronisation feature was conducted. From the perspective of this Office, there is a clear distinction between the two processes.

The friend finder feature following the upload of an address book as described earlier is intended to be a user-driven process with FB-I acting as a data controller for the uploaded data until such time as the recipient of an invite expressly asks not to receive further invites and at that point no further processing or association of their email address details takes place unless the person decides independently to join Facebook.

The Facebook iPhone application has two closely related features, contact synchronisation and find friends. Both of these features are accessible by pressing the same button, in the top right hand corner of the "Friends" screen in the iPhone app. If a Facebook user enables the contact synchronisation feature of the Facebook iPhone app, then if there are any existing Facebook users in the synchronised contacts, these will be suggested as people you may know. The existing Facebook users are presented both as a separate list under "Find Friends" in the iPhone app and also may be presented in the "People You May Know" section of the Facebook web page.

The synchronisation process without further action by the user, i.e., without engaging with the friend-finder tool, is a separate service and those synchronised email addresses should not be used for friend-finding purposes. In these circumstances FB-I is solely acting as a hosting service on behalf of the individual user and does not make any use of the data without the user's consent.

On this basis, the Team examined whether any material distinction was made within FB-I as to how email addresses synched in this manner are processed. In conducting this examination we noted information provided by FB-I to a user synching their device such as an iPhone. The user is informed that synched data may be used for friend-finding purposes, but we consider this service to be materially different to the upload address book feature above. This is respected by Facebook and it is only when a user after synching chooses to take the additional step to find friends that synched contact details of non-users are used for friend finding purposes.

In response to a specific element of the complaints, we are however satisfied that, aside from storage of such data for its users, no additional use is made of telephone numbers or other contact details uploaded as part of the synchronisation feature. FB-I only processes email addresses for friend finder purposes.

We are also satisfied that if a user chooses to delete their uploaded contacts that they are in fact deleted.

Where a user chooses to synch their contact information from a mobile device, such information is transmitted in plain text regardless of the state of the secure browsing setting. This is not an issue within Facebook's control but users should nevertheless be made aware when choosing this option.

Synching can be disabled at any time through the iPhone app which is the application chosen for testing purposes. 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. Again it should be clear to users that disabling synching is not sufficient to remove any previously synched data.

An additional issue identified was that selecting the "remove data" button having only synched data and not activated the friends finder feature did not appear to actually delete the data from Facebook just remove it from the phone. However, this matter was tested as outlined at section 3.4 of the Technical Analysis Report and it was established that the data is in fact deleted. The fact that it is not apparent to the user how to manage their synchronised contact information is a shortcoming in the user interface that we expect FB-I will resolve but it is not explicitly a data protection issue.

Uploaded contact information can be removed via the "remove all your imported contacts" link on the "Manage Invites and Imported Contacts" page within Facebook. This is the same process to be followed when contacts are imported from any source. However, removed contacts will be re-imported automatically unless the user turns off syncing in the Facebook iPhone app.

3.11.6 Business Upload

This Office also carefully examined the feature available on Facebook for a business to upload up to 5,000 contact details for invite purposes when launching or updating a company or business page. A number of issues arise for examination in relation to this feature. Firstly, the invite messages sent by such businesses do not fall to be considered under the household exemption discussed elsewhere in this report as they are sent by a business to what are stated to be its customers or contacts. Under Irish law[29] such messages may be considered as marketing messages which the relevant business would be considered to either have sent or caused to be sent and therefore the relevant business has a responsibility to ensure the messages are sent only to individuals who have given their prior consent to marketing (or have not opted out of receiving marketing messages where the email address is a business address). FB-I noted that as a measure to prevent Page administrators from sending messages to individuals located in the EU, it has geoblocked the major EU domains so that messages from Pages cannot be sent to the vast majority of EU users or non-users. In this respect it is noted that Facebook takes the additional precaution of highlighting to any business uploading contact details that there is a requirement for consent. The Page administrator must affirmatively indicate by checking a box that they have consent from the recipient to send a marketing message. The requirements of Irish law in this area are in fact very specific. Facebook also provides a link to additional information for Page administrators to read to ensure their messages meet the requirements of the law. The highlighting of the requirement for consent is to be welcomed but it is suggested given the importance of this issue that FB-I would wish to re-inforce this message and adopt a zero tolerance policy for any entity against whom it receives a sustainable complaint. As this Office is satisfied that FB-I has separate responsibilities under SI 336 of 2011 by providing a means for such messages to be sent we fully expect that it will be taking this matter seriously. FB-I has undertaken to bring forward appropriate measures in this area. These measures will be reviewed in July 2012.

A second issue is that given the requirement for consent to send an invite, a business while uploading a file of contact addresses to which it intends to send invites can be expected to remove certain addresses from the invite list which do not meet the stringent criteria. Any such removed addresses while uploaded cannot be further used for friend-finding purposes as it is not credible to suggest that the business is in a position to obtain consent for this purpose.

Finally in this area, this Office received a complaint from an individual who had received a friend invite via SMS. Unfortunately the opt-out mechanism which the person wished to use was not operating at the time and they were unable to do so. The ability to send friend invites via SMS was only recently introduced by FB-I and it was of some surprise to this Office that a feature such as this was available in the EU given the specific laws laid down under the ePrivacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) and as transposed in

[29] SI 336 of 2011 (http://dataprotection.ie/viewdoc.asp?m=l&fn=/documents/LEGAL/SI336of2011.pdf)

domestic law (SI 336 of 2011). FB-I explained that this feature was introduced in response to a demand in emerging markets where SMS messages as a means of joining Facebook are a significant and preferred channel for new members joining. The service only allows one invite to be sent by SMS at a time and requires that the user sending the invitation manually types in the recipient's phone number. FB-I stated that it has rectified the issue that arose in relation to the failure of the stop (unsubscribe) command.

FB-I in response has indicated that it acts as a facilitator of the SMS invitation sent by a user, that the user can only send one message at a time by typing in the phone number of the recipient, and the message has a Stop function. FB-I indicated that as soon as it learned that the Stop function was not working, it disabled the tool in the EEA. The tool will not be re-enabled until the function is working properly.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.		
	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.	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, 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.	End of Q1 2012.

	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.	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.	End of Q1 2012.
	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 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.	End of Q1 2012.
	We confirmed that passwords provided by users for the upload of contact lists for friend-finding purposes are held securely and destroyed		

3.12 Tagging

3.12.1 Complaint 3 – Tagging the complainant stated that friends on Facebook have the facility to 'tag' photos of another user (friend) and display them on their Facebook page and within the 'news feed' section. The complainant contended that Facebook does not provide an option to users to prevent them from being 'tagged' and that the 'tagged' item is on their Facebook page before they are aware of it. The complainant stated that the only option available to the 'tagged' user is to subsequently remove the 'tagged' item after it has appeared and, as the photo is automatically available to the user's friends, the content may be of embarrassment to the user.

The complainant also contended that if the user decides to remove the 'tag' it is not deleted and is retained in the background by Facebook. This aspect is dealt with elsewhere in this report.

The complainant considered Facebook to be in breach of data protection legislation as the data subject has not provided consent to have their photo 'tagged'.

In response to the specific issue of 'tagging', Facebook indicated that it has recently introduced a feature which allows users to approve or remove 'tags' before they are posted on their profile. Facebook stated that it has always has and continues to provide the option for users to remove previously 'tagged' items.

3.12.2 Analysis

The ability to apply tags is not limited to pictures or indeed friends. 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. In fact as tags generate an automatic notification to a friend they are used by many members as an automated means to notify a friend of something via the tag even if the content is completely unrelated to that person. In the Retention section of this report we have outlined the measures that will be introduced to allow a user to delete such tags subsequently if they wish to do so.

For those members who do not wish to be tagged at all, it is the case that at present there is no ability for them to express their preferences. However, a user can stop another individual user from tagging him or her by blocking that individual user. While preventing the tagging of yourself would mean that you would be less likely to become aware of a picture, post or comment in which you are referenced, 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.

FB-I's Response

Tagging is core activity on Facebook and has been positively received by Facebook users, especially as Facebook develops tagging in new ways in order to give users more means for connecting, sharing, and communicating. In contrast, there is generally no easy way for people to learn when someone has commented about them on the internet, 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 have much greater protections. They always receive notifications when they have been tagged and they have always had the ability to un-tag themselves. Tagging enables users to get immediately informed when their friends mention them in a post or a photo. It gives them 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 an assertion in which they're mentioned. As tagging has expanded, Facebook has been sensitive to those users who may want more control over the process and further added the ability for users to preapprove tags before they appear on their Timelines (formerly, profiles). Thus, Facebook ensures 1) notice of all tags to users; 2) the ability to require prior notice of all tags; 3) the ability to un-tag; and 4) the ability to simply block it from appearing on the user's own Timeline. Facebook firmly believes that it has struck the right balance in terms of product development and user control. Based on this Office's recommendation, FB-I will examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I will examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review	In advance of July 2012

3.13 Posting on Other Profiles

For active users of Facebook, posting comments, updates or content on their own wall or that of a friend is a part of their everyday use and enjoyment of the site. Due to a change made last August in which such posts can be made, users can choose the privacy setting for each piece of content they post on their own profiles at the time of posting. Visitors to the user's profile can also now see the privacy settings of the user's posts and therefore what the audience will be if the visitor decides to comment on a post. However, visitors will not immediately see the user's visibility setting for direct posts by visitors on the user's wall. Once a post is made, however, the visibility setting appears and visitors can see the audience for their post. At that point, a visitor can now choose to immediately delete their post if they have any concern about the setting in place at that time.

The precise way in which such posts operate from a privacy perspective was the subject of **Complaint 6 – Posting on other Peoples Pages from Europe-v-Facebook.** The complainant stated that when a user makes a comment, both the comment and the actual name of the person making the comment are visible. The complainant contends that the person making the comment is under the impression that he is simply sharing the comment with his own friends, but in actual fact, the comment made is subject to the privacy settings of the other user and may be available to a much wider audience – it could be restricted to friends only, but equally, could be viewed by everyone on the internet, including search engines.

FB-I advises users in its Data Use Policy that *"When you post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings."* The issue for the complainant was that there was no transparent notice provided to the member making a post to indicate the categories of users that would be able to see the comment. Subsequent to the submission of this complaint, Facebook changed the way in which posting works to provide transparency to users about the visibility of posts to which they might add a comment. The complainant welcomes this increase in control but reasonably pointed out that if the member on whose profile the post was made subsequently changed their settings to expand access to the post then the other member's post on their profile would be equally accessible. Additionally the complainant pointed out that there is no information displayed as to the settings on a member's profile if there is not already a post there and that even where the settings are displayed that can be somewhat oblique where for instance they only indicate "custom settings" or "friends of friends" and don't therefore provide any precise information on which to make a judgement as to whether to submit a post to that page or not.

FB-I does not share the complainant's view that a user commenting on a post on another user's page would assume that the comment would be subject to anything other than the other user's privacy settings. It has pointed out that in the new profile called Timeline, the setting in the post box expressly states that the privacy of the post is governed by that user's settings.

Regarding the lack of transparency for those making a comment on a post, Facebook highlighted two items from their Data Use Policy which states:

Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it.

And:

When you comment on or "like" someone else's post, or write on their Wall, that person gets to select the audience.

Additionally, FB-I stated that with Timeline, visitors to a user's profile can now see the privacy settings of posts on which they might want to make a comment.

3.13.1 Analysis

In assessing this issue account must be taken of the inherent social nature of Facebook and the close interaction and relationship that exists between members who have chosen to accept each other as friends. In this respect much as in the world that exists outside social networking, friends have to first of all be expected to act reasonably with each other and where one friend does something that offends or otherwise surprises another friend then the normal way to resolve such an issue is for discourse between those friends. Undue interference by or recourse to the authorities, in this case Facebook, can sometimes serve to make an issue worse. With this in mind Facebook has in recent months introduced enhanced tools, which are described elsewhere in this Report, for friends to raise concerns with each other or via another trusted friend about behaviour on Facebook as an alternative to invoking Facebook itself. The introduction of these tools are to be welcomed from a data minimisation perspective as solely providing tools for complaint to Facebook increases the amount of data held on members submitting and the subject matter of complaints.

It is clearly also in Facebook's interests that members feel able to post on other member's pages or use the many other tools available that allow them to express themselves or interact on Facebook without a doubt on their parts as to what will actually happen to that post. In this respect the data protection concern to ensure that an individual has full information when making a post and the interest of Facebook to encourage use of the site coincide. A difficulty however in this area as Facebook has correctly pointed out in reply is that it is not possible to reveal personal data about the person on whose page you are posting without running into data protection concerns. The complainant has suggested that some information be provided to the poster about number of friends etc to whom a post would be visible. This could perhaps be achievable by informing the poster that it would be visible to >100 people or <100 people when posting. The complaint also highlights an issue if privacy settings are subsequently changed that make a post that was initially restricted available to a broader audience. A potential solution in this area might be the triggering of a notification to the poster of the change with an ability to immediately delete their post if they are unhappy. Based on this Office's recommendation, FB-I will examine the broader implications of the suggested approach and having done so will engage further on this issue in the July 2012 review.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I will examine the broader implications of the suggested approaches and having done so will engage further on this issue in the July 2012 review.	In advance of July 2012

3.14 Facebook Credits

3.14.1 Risk Operations & Payment Operations

Risk Operations has a global remit and is charged with mitigating financial losses or compliance breaches suffered by FB-I by proactively investigating potential fraud by users. Payment Operations is also a global team handling the purchase and management of "Facebook Credits" which is the particular focus of this section. There are 23 staff based across these two teams.

Since July 2011 any third party game available via the Facebook Platform that requires a form of payment to purchase virtual goods, must use Facebook Credits as the required currency. Previously such payments were managed in a number of different ways but now all such payments are handled by Facebook. FB-I indicated that Facebook Credits are the global currency of the Facebook Platform and were introduced to protect its users from payment fraud and to provide an effective payments solution that can be integrated into apps. It also stated that Facebook Credits allow users to have greater confidence in their payments on Facebook and enable developers to focus on their unique offering, rather than the difficulty of implementing a payment solution.

Given that it is FB-I's view that all third party applications are separate data controllers from it, a detailed analysis was conducted as to the precise legal status of FB-I when it processes these payments as a standard analysis of an entity providing such a service would generally be considered to be acting only as a payment processing agent on behalf of each third party application.

The operation of Facebook Credits can be broken into three stages: the opening of an account for Facebook Credits and transfer of user funds to Facebook; the use of those funds by a user to purchase items on the Facebook platform; and the redeeming of credits for "real world" currency by an app developer.

Stage 1: All users outside of the US and Canada purchase Credits directly from FB-I via the "Payments" function in their Account Settings.

Each Facebook Credit is worth USD 10c. The actual price paid for Credits will fluctuate based upon the dollar exchange rate.

Stage 2: FB-I accepts payments via PayPal on foot of agreements which it has in place. These agreements were provided on request and were considered to be in order. Other modes of payment (particularly cards) are processed on behalf of FB-I by an Irish established payment institution regulated by the Central Bank of Ireland.

Technically, purchases on Facebook via Facebook Credits are implemented via the Facebook Credits API. Detailed technical information in connection to this API can be found here.

If a user chooses to make a payment in an app they do so by pushing a "purchase" or similar button within the app. This button leads to the app making an API call to FB-I. This call provides FB-I with the details of the item which the user wishes to buy, including its price. FB-I, and not the app, then displays the relevant offer to the user and completes the transaction.

Stage 3: Developers can redeem their Credits for payment in US dollars at the end of each bimonthly period. Redemption is made either by PayPal or by funds transfer to a verified bank account.

FB-I's position is that while FB-I is offering a payment solution to app developers it does not act as a data processor on their behalf. FB-I is the data controller with respect to the Facebook Credits personal data including data relating to quantum of credits held by a user and the payment methods used to purchase these. This classification flows from the facts (i) that the relevant personal data (i.e. how many Credits are held by the user and the mode of purchase of Credits) is, at all times, held by FB-I and (ii) by the fact that FB-I has set up and administers the payment processes directly with users.

The app has no control over such personal data and has no right, either under contract or otherwise, to access such information. App developers merely provide Facebook with the price of the item that a user wishes to purchase and the identity of the relevant user. Should the user choose to complete the transaction, he or she does so with Facebook.

Credits are governed by Statement of Rights and Responsibilities and its ancillary agreements, which include the Platform Policies, the Facebook Credits Terms and the Payment Terms. All users and developers outside the US and Canada enter into these agreements with FB-I Limited. It is FB-I Limited, and not Facebook Inc., which offers Credits on a worldwide basis (excluding US and Canada) and which is entitled to enforce Facebook's global contractual rights with regard to Facebook Credits aside from those rights concerning US and Canada. From an internal Facebook perspective, the Payment Operations division of FB-I has global responsibility for Facebook Credits (excluding US and Canada).

FB-I maintains full control over the manner in which Facebook Credits are offered. While FB-I do facilitate developers in receiving payment via Credits, it does so on our terms, terms which it is contractually free to change at will.

We examined a workstation in Risk Operations and viewed several suspect fraud cases. The level of detail appearing for each user account was significant. This is an issue which is addressed in detail in the subject matter section on Retention. The detail contained included activity on the Facebook account over a number of years including the IP address of every access to the site by the user and the details generated by a named cookie. FB-I explained that this information helped indicate to the Team unusual patterns of access for a particular user which assists in assessing a potential fraudulent transaction. A member of the Risk Operations Team worked through the steps involved in assessing suspected fraud cases and demonstrated the reallocation of credits to the user if there were reasonable grounds to believe the user's account had been compromised by a third party.

3.14.2 Analysis

This Office can accept based on our examination of the actual operation of Facebook Credits that FB-I does act as a data controller in the provision of the 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 in this respect and that furthermore information generated in the context of their use of Facebook

Credits is linked to their account. In this respect while it is accepted that there is comprehensive information available to users via the payment terms page as to how Facebook Credits are managed, there is only one reference to Credits in the Data Use Policy and accordingly it is recommended that the information available from here as to actual personal data usage in this context be significantly expanded.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I will be adding information to this effect in the Data Use Policy and it is launching a privacy policy for its payments systems in approximately six months.	End of Q1 2012.

3.15 Pseudonymous Profiles

The Article 29 Working Party Opinion on Social Networking[30] and a number of resolutions drawn up at international data protection and privacy conferences have called for social networking sites to allow their members to adopt pseudonymous identities in terms of their virtual identity within their social network of choice. This model is similar to the operation of discussion boards etc where individuals can post under a username that does not reveal their identity. The background to this position is grounded in the perception of the impact on an individual's right to privacy if they are denied the right to act online under a pseudonym rather than under their real identity. An example might be protestors in a country having the ability to communicate with each other without their identities being obviously known to the authorities which may tend to inhibit them. Although experience would tend to suggest that this does not in fact happen.

The requirement to provide verifiable information upon sign-up is accepted. It is the right to have the opportunity to act in a social network under a pseudonym where concerns have been raised. The Article 29 Opinion states

> "SNS should consider carefully if they can justify forcing their users to act under their real identity rather than under a pseudonym. There are strong arguments in favour of giving users choice in this respect."

We have noted that Facebook permits individuals to adopt usernames but these do not replace or override the actual name of a member, they are a tool to be used as outlined by Facebook in its Data Use Policy:

> ***I. Information we receive and how it is used***
>
> *Usernames and User IDs*
> *A Username (or Facebook URL) is a custom link to your profile that you can give out to people or post on external websites. If you have selected a username, it will always appear in the URL on your profile page. If you have not selected a username, then the URL on your profile page will contain your User ID, which is what we use to identify your Facebook account.*

Facebook's **Statement of Rights & Responsibilities**[31] states

> *Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:*
>
> *You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.*

[30] 1) WP 163 Opinion on online social networking, June 2009.

[31] http://www.facebook.com/terms.php?ref=pf

You will not create more than one personal profile. If we disable your account, you will not create another one without our permission.

You will not use your personal profile for your own commercial gain (such as selling your status update to an advertiser).

You will not use Facebook if you are under 13.

You will not use Facebook if you are a convicted sex offender.

Finally, the Team also noted Facebook's Safety Centre[32] which is a dedicated web area for teenage members of Facebook and their parents and teachers.

The Importance of Being You

Facebook is a community where people use their real names and identities, so we're all accountable for our actions. It's against the Facebook Terms to lie about your name or age. Help us keep the community safe by reporting fake profiles to Facebook if you ever see them.

FB-I indicated that Facebook's real-identity culture is one of its core values. Over 800 million registered users have established connections and shared information with friends on Facebook relying on the understanding that their friends are who they say they are. Importantly, the safety, security, and integrity of the Facebook service depend upon the authenticity of Facebook accounts, i.e., that they belong to real people who represent themselves authentically. FB-I further indicated that Facebook's core mission – to make the world more open and connected – relies on fostering a genuine and trustworthy social environment in which people feel comfortable communicating and sharing. FB-I stated that all of the building blocks of the Facebook Platform as it exists today rest on the foundation of a real-identity culture. FB-I stated that it strives to replicate real-world social norms in an online environment by emphasizing the human qualities of conversation and sharing. Attaching people's real names to their communications and actions on Facebook promotes accountability and responsibility. In fact, FB-I reported that Facebook receive tens of thousands of complaints each day from users who believe that another user on the site is inauthentic, and who demand that Facebook take action to protect this core aspect of the Facebook community. FB-I also noted that the real-identity requirement is integral to user safety on the Facebook Platform and a fundamental component of the security measures it implements. The safety, security, and integrity of the Facebook Platform would be compromised significantly without such measures. Many of our safety and security measures involve removal of inauthentic accounts -- from spammers and phishers to individuals who are abusing the Platform and do not want to be discovered. FB-I reported that the vast majority of accounts that it disables for being inauthentic are associated with behaviors that violate other terms of use, like bullying and harassment. Finally, FB-I stressed that without the requirement that individuals present their real identities, Facebook would be an entirely different business; its defining mission would be unfulfilled. It simply would not be Facebook. FB-I maintained that for Facebook to abandon its core principle of real identity would require the dismantling of the existing social network and Platform and the creation of a new social network and Platform.

[32] https://www.facebook.com/safety

FB-I described the substantial efforts of its User Operations Team to investigate potential fake and imposter accounts created by adults to make contact with teenagers, created by teenagers to bully other teenagers, and created by adults to harass others. Should fake identities be common place, more social interaction with fake accounts would occur before the targeted user became suspicious of the intentions of the creator of the fake account. This is particularly important when it comes to protecting children in the online space. Groomers are adept at identifying, targeting and isolating children. One of the main models of groomering behaviour is establishing whether a child will conceal the interactions from a trusted friend, teacher, or parent. By ensuring that everyone who comes into contact with this account will be suspicious of its fakeness we convert the online space into a community watch program.

Child exploitation, threats, stalking and other serious offences that Facebook fight are committed through the use of fake or impostor accounts, as the offenders obviously want to conceal their true identities.

Moreover, the use of real identity often helps in tracing the real person behind an offender's profile. Under the real name policy, Facebook is aware of the declared identity of the users and reporters as well as their declared ages. During investigations, Facebook looks at a number of surrounding details which highlight red flags in terms of online behaviour. When users are representing themselves legitimately there is no clash between these facts and their declared identity. However, when users are being deceptive as to their identity they are easily identifiable by the discord struck between these signals. These elements enable Facebook to expediently identify suspicious user behaviour.

3.15.1 Analysis

Facebook has made a definitive policy position not to allow pseudonymous identities. We sought clarification from FB-I as to the justification for this policy which is outlined above. We are satisfied that FB-I is not contravening data protection law in Ireland by offering a free service which requires real names and identities. If a user feels more comfortable with a service which provides pseudonyms then a user can use an alternative service. Without prejudice to the position held by any other data protection authority, we consider that FB-I has advanced a sufficient rationale for child protection and other reasons for this policy position and do not consider that from an Irish data protection law perspective that there is sufficient justification as to require that FB-I adopt a different policy.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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		

3.16 Abuse Reporting

We have noted that Facebook provides its users with a variety of ways to report abuses on the site. Users can go to the Help Centre and find pages of information about abuses to report. FB-I also has contextual reporting buttons on every page and associated with every piece of content. On every profile, there is a report link; on every photo there is a report link; and on every advertisement there is a way to report it. There is a means to report abuses included on every profile, photo and advertisement.

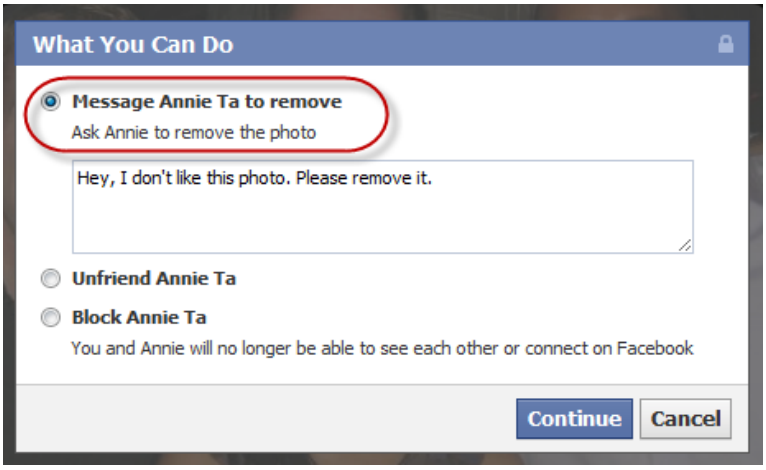
In addition, Facebook has also developed what it terms an innovative tool called "social reporting" that helps people directly notify others of content they want removed from Facebook, and that gives people more reporting options should they ever be concerned about content they encounter on Facebook.

FB-I has indicated, for instance, that if a friend posts content about a user that the user does not like, the user can use the social reporting feature to ask that friend to remove it. Because the reporting process is both private and similar to the kind of communication that two people might have in the offline world, FB-I reports that it has proven to be a hugely successful content removal system.

Moreover, social reporting has also proven an extremely effective mechanism to combat bullying and other abusive behaviour. Through Facebook's social reporting tool, people also have the option to block communication with others, report content that may be in violation of our policies to Facebook for removal, or even send a copy of abusive content to a trusted friend or adult who may be in a position to help address the person's concern.

As an example, if a user objected to a photo their friend posted because it was unflattering, the user could use the social reporting tool to indicate that they don't like it:

Next, the social reporting tool would offer options for addressing the problem, such as sending a message to the user who posted the photo to ask her/him to remove it.



Depending on the nature of the problem, the tool would present other options, such as contacting an authority figure or friend to help the user work out the issue in person. (Where appropriate, of course, the user also could report the photo to Facebook directly.)

Facebook provides its users with facilities within its Help Centre to report on instances of abuse they may encounter, for example, pornography, hate speech, threats, graphic violence, bullying and spam. A user can submit reports under a range of headings:

- Report a fake or impostor profile (timeline)
- Report a photo or video
- Report someone's timeline cover photo
- Report a page
- Report a message
- Report a group
- Report an event
- Report a question or post in Facebook Questions
- Report a post
- Report an ad

In order to send a report, Facebook advises the user (via the Help Centre) on how to complete reports on the above items. In some cases, for example where the user wants to report a bullying issue or offensive content, Facebook prompts the user to click on a dropdown menu (⚙ ▾)

beside the offending item which then leads the user into the reporting option. Similarly, if a user is reporting a fake user account, the user is directed to the report/block option from the dropdown menu ( ) on that user's Facebook page.

However, the user is not provided with any information as to how long the report will be retained or if it is to be further processed in any way. It is also unclear as to the type of response or feedback a reporting user receives from Facebook. Facebook's Help Centre does advise that "*the person reported is not notified of the identity of the person who made the report.*"

13.6.1 Accessibility of Options

We examined the accessibility of options available to a user who wishes to report an issue to Facebook. It is considered that it is straight-forward for a user to locate the 'Report Abuse' options via the 'help' dropdown option on the user profile page and within 2 mouse clicks is within the 'Report Abuse or Policy Violations' of the Help Centre.

Each of the headings provided comes with instructions on how to use that particular option, including the location from which the user may exercise that option (for example, homepage). Clicking on a heading provides a list of typical questions related to that subject, though the user may also use the freetext 'Search the Help Centre' option at the top of the screen if s/he is unsure of what heading is most appropriate to their particular issue.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
Abuse Reporting	We are satisfied that FB-I has appropriate and accessible means in place for users and non-uses 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.		

3.17 Compliance Management/Governance

3.17.1 Compliance Management/Governance

As detailed in the General Audit Section of this report, FB-I was assigned increased responsibility for all users outside of the USA and Canada in September 2010. A focus for our Office therefore throughout the audit was on establishing that FB-I had in place the procedures, practices and the capacity to ensure that personal data for which it has a responsibility is handled in accordance with data protection requirements. It is clear from the recent FTC settlement that Facebook will have in place a comprehensive programme for ensuring that it meets user expectations in relation to privacy. This programme will also ensure that privacy considerations are embedded into product development.

The substance of the Facebook presence in Ireland via FB-I is apparent from this Report and it is clear that senior staff in Dublin play a substantial role in the handling of user data by Facebook. We have acknowledged that meeting the compliance responsibilities for the day to day handling of user data in an environment such as Facebook 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.

An organisation such as FB-I with a responsibility for such a significant volume of personal data must also be able to demonstrate that it has relevant governance structures in place to be fully accountable for how it handles and manages the data involved. Accountability for personal data handling is already part of some international data protection frameworks. It is implicit in the current EU framework and is fully anticipated to be an explicit requirement in the future EU data protection framework. This Office examined the capacity of FB-I to meet this responsibility. From a data protection perspective it is necessary for FB-I to be able to demonstrate that it is in a position to take responsibility for ensuring that data protection and privacy laws are respected in the day to day handling of data and importantly during the development and roll-out of new products and features. The formal task of this Office is to ensure that FB-I is compliant with the requirements of Irish data protection law which in turn transposes the requirements of the common EU data protection legal framework. In practice, we seek – and have sought with FB-I – to go beyond mere compliance towards a best-practice approach.

3.17.2 Complaints Handling in FB-I

Some time ago FB-I established a dedicated casework team in Dublin as part of the user operations team to deal with complaints from users in relation to privacy issues. The team also deals with and prioritises direct contact from data protection authorities on behalf of individuals with such privacy concerns. This is done via a dedicated address. In the experience of this Office, where complaints or queries are bought to the attention of the casework team, they are dealt with expeditiously and the issue at the root of the contact resolved. This team is a practical and ongoing demonstration of FB-I meeting its day to day responsibility for handling user data in a compliant manner.

3.17.3 Data Transfer

As outlined earlier this Office sought and assessed all the contractual arrangements entered into by FB-I and Facebook operations throughout the EU and outside as appropriate to ensure that all required conditions for the processing of personal data were met. Transfer to the US is handled by way of the Safe Harbour provisions and an explicit contract between FB-I and Facebook Inc. Transfer from FB-I to territories outside of the EU is handled by way of processing contracts entered into by FB-I and/or Facebook Inc., and the Facebook entity in the importing territory if it has a responsibility for processing user data. Access to user data by Facebook entities throughout the EU as described earlier in the report is handled by way of data controller to data processor contracts which are consistent with the requirements of Section 2C of the Data Protection Acts. FB-I indicates that such access only takes place in very limited circumstances under controlled conditions in the context of the marketing/advertising and limited engineering functions performed by these Offices.

3.17.4 Third Party Contractors

FB-I does not at present make substantial use of third party contractors to process personal data on its behalf or that would have a potential to access personal data in a security or IT support capacity as an example. Where such contracts are in place they were sought and provided and were also considered to meet the requirements of Section 2C of the Acts.

3.17.5 Governance

As stated above, the position of this Office is that FB-I must be in a position to demonstrate its accountability for applying data protection requirements to its handling of personal data. While the focus of the audit was the processing of user personal data, we also took the opportunity from a compliance perspective to examine the frameworks in place to ensure that legal requirements in relation to non-user data are in a position to be met. In relation to employee data, while it was not examined in detail we did however note appropriate contractual provisions and policies to indicate that data protection obligations to employees are understood and implemented.

During the audit it was established that FB-I engages in direct marketing activity focused on acquiring additional business customers on the site and utilising the advertising capabilities of the site to reach users. As this area traditionally accounts for a large volume of complaints to our Office (none in relation to FB-I) and where Irish law[33] which has transposed the ePrivacy Directive imposes very strict obligations for all such contact, including to businesses, it was decided to examine this area in detail.

FB-I operates a call centre in Spain via a third party service provider which contacts businesses in the EMEA region that have been highlighted as prospective leads on behalf of Facebook. It has also engaged with another third party to make calls and send marketing emails on its behalf using lead information generated by that party. This Office was satisfied that the calls and emails were made and sent on behalf of FB-I respectively. In this respect it is our position that all such calls must comply with Irish electronic communications marketing law. In particular, no calls must be made to a business on a number that is listed on any national opt-out register not to receive unsolicited calls. Where the business indicates that it does not wish to receive any future such calls it must be entered on a do-not call list held by or on behalf of FB-I. There must be procedures

[33] http://www.dataprotection.ie/documents/legal/SI336of2011.pdf

in place to ensure that all such requests are complied with. For calls to mobile phone numbers, all such calls must have the prior consent of the recipient to receive a marketing call from Facebook.

The sources for the contacts were either direct customer contact with Facebook which does not give rise to the same level of focus and lead lists generated by a third party supplier. FB-I fully accepted its responsibility for its use of the data and outlined its procedures for refining and cleansing its usage.

The contract in place with the third party agent in Spain was examined and contained appropriate clauses to comply with Section 2C of the Acts. FB-I also indicated that only fixed line numbers receive what would be termed unsolicited calls by the team[34]. In light of the above compliance obligations and on foot of the audit, additional steps were taken by FB-I to ensure that businesses receiving unsolicited marketing calls had not objected to such calls. In this respect FB-I indicated its understanding that the third party agent had not received any requests to opt out of future calls but was undertaking work to ensure that the calling system could fully record any such preferences if received. FB-I is currently improving its salesforce system and is creating a more prominent section "Do not Call / Opted-out users" to identify more clearly and quickly individuals who do not wish to be contacted by phone. FB-I also put in place additional training for the third party agent and other internal sales staff to ensure future compliance with this provision. A copy of FB-I's new training materials were made available to the Office and were considered satisfactory.

FB-I's purchase of lead data for businesses from a lead list supplier was also examined. The agreement in place is considered by FB-I to constitute a data controller to data controller agreement. The agreement places an obligation on the supplier to comply with applicable laws and to ensure that the disclosures of personal data pursuant to FB-I are lawful and that the consents of the underlying data subjects exist. The provisions of the contract in place are considered in order.

In relation to email marketing the relevant requirements under our electronic privacy law are that a business recipient be given an ability within the received email to opt-out from any future contact. As all marketing contact from FB-I is focused on businesses this should meet most requirements. However, the requirement in relation to individuals is that the entity (or another party on its behalf) direct marketing its products must have collected a valid consent. It is not considered possible for a generic opt-in consent referring to the receipt of electronic communications generally to be relied-upon. Where an email is sent advertising a Facebook service, even by a third party which generated a lead, then FB-I has full responsibility for ensuring that the recipient, if a natural person, has agreed to the receipt of electronic marketing communications from it, with some exceptions for business-to-business email, and in all cases that the communications contain a valid means to opt-out which are respected if exercised.

3.17.6 Analysis

Since the conduct of the onsite element of the audit, FB-I has put in place a number of enhancements to the conduct of direct marketing campaigns via system changes and training. These are to be welcomed as a strong indicator of the commitment of FB-I to ensuring that Irish

[34] Mobile numbers are only called when a customer or potential customer has explicitly requested to be called on its mobile number

data protection laws are respected in practice. However, it was also clear that the compliance requirements for the conduct of such direct marketing had not been fully understood by certain FB-I staff members engaged in marketing in advance of the audit commencing. As noted above, while not relating to the processing of user data, this area was subjected to a detailed focus to identify how compliance was handled within FB-I and accordingly we would conclude that there is room for improvement generally. In this case 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.

3.17.7 Privacy review for products

We sought information from FB-I as to how data privacy is embedded into product design and roll-out. FB-I in response, inter alia, stated the following:

> *Recently, a Chief Privacy Officer of Product was appointed, a new role that signals Facebook's commitment to embracing a privacy-by-design method of product review rather simply a legal review. As well, a Chief Privacy Officer for Policy has recently been appointed to ensure that privacy is even more deeply embedded in our policy development moving forward. Therefore, the previous privacy review process, described below, will be enhanced by these new objectives.*
>
> *We organise reviews of new products and features around a product roadmap - the legal department uses this roadmap to outline and organize its review of upcoming products. That roadmap identifies the products or features being developed, the project manager (PM) and the timeline for the launch. The review process begins with an initial assessment of issues based on the information available in the roadmap.*
>
> *Then, based on launch schedules and issues spotted, internal meetings are scheduled to provide the legal team with an overview of the proposed product or feature. This often is a multi-step process, where legal works with the PM to track tasks and includes vetting product features with other internal lawyers (e.g., specialists, regional counsel) and outside/local counsel, as needed.*
>
> *Legal works with Irish outside counsel and outside counsel from other European countries, as well as, in some instances, outside counsel from additional countries, to ensure compliance with all applicable laws, as well as to consider any potential sensitive issues.*
>
> *After legal's thorough review and analysis is complete, the PMs are presented with an assessment of any possible issues. The PM and legal work together to determine whether changes to the product or feature are necessary. Legal will continue to work with the PM to address compliance needs, specifically including special user education, Data Use Policy or Terms updates, or other notice that may be required. If such elements are warranted, legal and the PM work with a cross function team that develops these materials. Once ready and approved, these user-facing elements are introduced into the product experience.*
>
> *Next, the legal team conducts another separate review, including a review of mocks or actual demo version of the product or feature. The legal team then will go back to the PMs*

with follow-up questions and recommendations.

User operations (UO) is then organized to conduct tests on the proposed product or feature – to determine whether there are any surprising or unexpected behaviours or if there are any bugs in the system. UO will document their findings and present them to legal and the PM. Once outlined, the team will work together to resolve any issues, including filing tasks to execute any necessary changes.

The PMs will come back to the legal team once the next iteration of the product or feature is ready for another review or a final review.

Once the product or feature is far along in this process, FAQs and other help materials are developed to coincide with release of the product or feature. During this stage, the user experience is examined to determine where user education or notice should be presented to users.

Elements of this process are repeated, as necessary, during the initial product review cycle and even after launch, as changes or enhancements are made to the product or feature. Feedback from users and other interested parties is received as part of this post-launch review process and further refinements are made as necessary.

During the review process, the legal team routinely consults with our Chief Privacy Counsel and Lead Privacy Counsel for their input. Additionally, FB-I frequently consults with this Office prior to launch of products in the EU and has indicated its commitment to engage further in such discussions on a regular basis. FB-I indicated that it also previews new products to other DPAs and is likewise committed to continuing such conversations.

3.17.8 Analysis

As a first observation it can be assumed that the above processes as they relate to Facebook Inc will be under review and continuously assessed including by independent third parties under the terms of the FTC settlement. This is very much to be welcomed and given the high standards set in the settlement it can be expected that new products and features brought forward by Facebook Inc will have privacy considerations hard coded into them from the very outset. As social networks rely on personal data as their lifeblood for their continued success and innovation, one should not expect anything less. The issue for this Office to consider is what if any analogous or additional steps are required by FB-I to ensure compliance with Irish data protection law requirements. In this respect as acknowledged above, it is clear that in the last several months that FB-I has brought about a large number of data protection improvements for the users for which it is responsible. Additionally the policy casework team provides day to day expression of the commitment to handling privacy complaints from or about individual users.

There is however a remaining legitimate 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. The troubled introduction of the auto tagging/facial recognition feature within the EU in June 2011, which is addressed earlier in this report, is perhaps the best recent

example of the disconnect that existed at that time. As stated above FB-I has worked hard since that time to address this issue for the users for which it is responsible. This Office cannot accept a situation where the requirements of Irish data protection law and by extension European data protection law are not 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. We will fully assess the improvements made in this regard in July 2012 and will expect that by that time FB-I will have in place the procedures, practices and the capacity to comprehensively meet its obligations in this area.

FB-I indicated its intention to 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.

Recommendations

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	FB-I RESPONSE	TARGET IMPLEMENTATION DATE
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.	FB-I has implemented these recommendations and supplied the relevant documentation produced and training given to this Office.	Complete
	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 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.	We will fully assess the improvements made in this regard in July 2012 and will expect that by that time FB-I will have in place the procedures, practices and the capacity to comprehensively meet its obligations in this area.

APPENDICES

Appendix 1	Technical Report and Analysis
Appendix 2	Summary of Complaints
Appendix 3	Overview of Team Functions (Provided by Facebook Ireland)
Appendix 4	Structure of European Offices (Provided by Facebook Ireland
Appendix 5	Law Enforcement Requests (Provided by Facebook Ireland)
Appendix 6	Minors