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

Response to Complaint(s) Number: 12

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

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

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

1. In the submissions Facebook Ireland Ltd does in many cases **not responded to our complaints**, but produced arguments and submissions that are irrelevant to the complaints filed. It seems that Facebook Ireland Ltd is trying to "bypass" the arguments we entertained.

2. In the submissions Facebook Ireland Ltd does in many cases **summarize our complaints** in a way that does not reflect the content of our complaints. We do not know why Facebook Ireland Ltd has chosen this approach other then again "bypassing" the core of the complaints.

3. In the submission Facebook Ireland Ltd does not respond to the **legal arguments** that were submitted by us, but only focus on facts. The law is not cited in any of the submissions.

4. In the past 2 years Facebook Ireland Ltd has changed many functions. In the submissions Facebook Ireland Ltd does in many cases **mix the factual situation** throughout this time period. Our complains are usually separating facts and consequences before and after such changes.

5. In the submission Facebook Ireland Ltd does in many cases refer to the "**audit reports**". The basis for these reports is not public or independently verifiable. In many cases the DPC has only relied on unverified arguments by Facebook Ireland Ltd when making its assessment. Facebook Ireland Ltd is now relying on these findings, as if they were independently verifiable facts.

➔ **Therefore we recommend to consult our original complains, as amended by the "request for a formal decision" [DOWNLOAD] when analyzing the submissions from "Facebook Ireland Ltd".**

COMPLAINT 12 – DATA SECURITY

1 INTRODUCTION

FB-I takes security extremely seriously. The DPC recognised FB-I's efforts and accomplishments in this respect during the audit process.

1.1 Data Use Policy

In its Data Use Policy, FB-I informs users about security matters and about the Security Page, where users can find additional security updates from Facebook.

> *Security and bugs*
>
> *We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page. We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products.*

1.2 Security Page

On the Security Page, FB-I provides users with information about how to keep their information safe and secure both on and off Facebook and regularly updates users on security matters.

1.3 Help Center

The Help Center offers a comprehensive source of information to users. The section concerning security includes extensive information on 'Hacked Accounts', 'Known Security Threats', 'Security Tips', 'Extra Security Features' and 'Using Games & Apps Safely'.

1.4 Enhanced Security

In addition to the significant technical and physical security safeguards which FB-I uses to protect its users, Facebook provides a number of extra security features. Details of these features, and how they can be activated, are set out in the Help Center. Facebook's extra security features include:

- Secure Browsing – When a user has secure browsing (or https) turned on, FB-I encrypts the user's activity on Facebook where possible, making it harder for others to improperly access their Facebook information or activity.

- Active Sessions - The active sessions section of a user's Security Settings page shows a user a list of the recent times his or her Facebook account was accessed. Each entry includes a date, time and approximate location when signing in, as well as the type of device used to access the account. Users are also presented with an option to end any active session.

- App Passwords - App passwords are one-time passwords a user can use to log into his or her apps and help keep his or her Facebook password safe.

- Login Approvals - Login approvals are an extra security feature similar to login notifications, but with an extra security step. If a user turns on login approvals, he or she will be asked to enter a special login code each time he or she tries to access his or her Facebook account from a new computer or mobile phone.

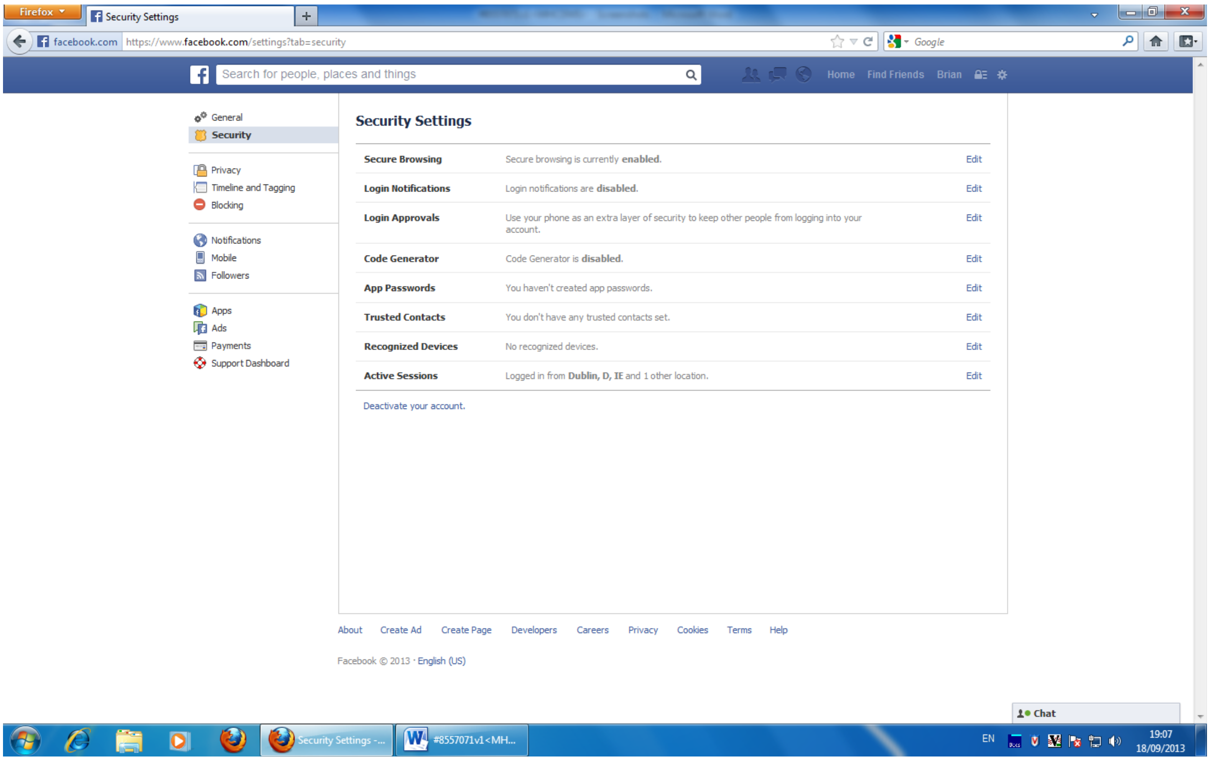
- Login Notifications – When a user turns on login notifications, Facebook will send him or her an alert each time someone logs into his or her account from a new place.

- One-Time Passwords – A user can use a one-time password to log into his or her account anytime he or she feels uncomfortable entering his or her real password on Facebook (for example, in a library or internet cafe).

- Trusted Contacts – Trusted contacts are people a user can reach out to if he or she needs help getting into his or her Facebook account (for example, if he or she forgets his or her Facebook password and cannot get into his or her email account to reset it).

1.5 Security Settings

Users can activate the extra security features from the "Security Settings" page of their Account Settings:



Security Settings

Secure Browsing	Secure browsing is currently **enabled.**	Edit
Login Notifications	Login notifications are **disabled.**	Edit
Login Approvals	Use your phone as an extra layer of security to keep other people from logging into your account.	Edit
Code Generator	Code Generator is **disabled.**	Edit
App Passwords	You haven't created app passwords.	Edit
Trusted Contacts	You don't have any trusted contacts set.	Edit
Recognized Devices	No recognized devices.	Edit
Active Sessions	Logged in from **Dublin, D, IE** and 1 other location.	Edit

Deactivate your account.

2 FACTUAL ASSERTIONS MADE BY COMPLAINANT

In the Original Complaints, the Complainant makes the following main factual allegations, which are reiterated in the Request for Formal Decision:

(a) "Facebook Ireland only seems to be encrypting passwords and credit card numbers."

(b) Statements in Facebook's terms and privacy policy "make it very questionable if Facebook Ireland is seriously protecting personal information. In fact, they are not even claiming that they are protecting it; they are straight out saying that they do not guarantee any security."

(c) "Even the most basic [app developer] provisions (such as providing some kind of privacy policy) are … not enforced by Facebook Ireland."

(d) Facebook is failing to take appropriate steps to secure applications.

(e) Facebook is failing to take appropriate steps to prevent the scraping of user data.

In the Request for Formal Decision, the Complainant continues to maintain his allegations, stating:

(f) *The 2011 Audit Report suggests that FB-I acted unlawfully by not having appropriate security in place.*

(g) *The audit "in no way tested or reviewed the proper functioning or even the existence of the controls"* and has not "*established any verifiable facts concerning this matter. It has merely relied on hearsay and absurd arguments.*"

(h) *The capabilities of the DPC's external expert are "questionable".*

(i) *"There was no proper limitation of access within the company on a 'need to know' basis."*

FB-I rejects all of these assertions, which are inconsistent with the position as set out in the Audit Reports.

3 AUDIT PROCESS

3.1 2011 Audit Report

The 2011 Audit Report delved into numerous aspects of Facebook's security in depth. Following extensive analysis, the DPC concluded that FB-I had appropriate security in place.

3.1.1 Focus on Security

At the outset of the 2011 Audit Report the DPC indicated the importance of security assessment during the audit process:

> *An assessment of security policies and practices including access control within an organisation is a standard feature of all audits conducted by this Office.*
>
> …
>
> *It was therefore incumbent upon this Office to devote a significant focus during the audit to assessing security issues*[1]

The 2011 Audit Report further noted the extensive resources which both the DPC and FB-I devoted to addressing security issues during the Audit:

> *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.*[2]

For the purposes of the 2011 Audit Report, the DPC appointed a technical expert to carry out an in-depth technical review of FB-I's systems and, together with a team of investigators, assist in thoroughly reviewing the security of data within FB-I.

3.1.2 DPC's understanding of the complaint

The Complainant's complaint was set out by the DPC at pages 106 to 107 of the 2011 Audit Report in the following terms:

> *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*

[1] Page 106 to 107 of the 2011 Audit Report

[2] Page 107 of the 2011 Audit Report

> *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.*

3.1.3 User-facing security

The DPC set out the following views with respect to FB-I's user facing security features:

> *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]

In addition, the DPC recognised the importance FB-I places on ensuring a robust system of security for user data. It stated:

> *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.*[4]

In reviewing the security of user accounts, the DPC documented the variety of features that users can themselves choose to avail of to provide additional security:

> *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.*[5]

Additionally, the DPC considered the usage of cookies by FB-I in the context of security. It was satisfied with the manner in which FB-I employs cookies to provide a more secure user experience and avoid malicious activity which might otherwise occur:

> *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*

[3] Page 107 of the 2011 Audit Report
[4] Page 108 of the 2011 Audit Report
[5] Page 108 of the 2011 Audit Report

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.[6]

3.1.4 Corporate Security

The 2011 Audit Report further set out, in summary form, the wide variety of security features deployed by FB-I:

- *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 compliance pertaining to the storage of customer financial data has been presented.*[7]

3.1.5 Employee Access to User Data

FB-I has comprehensive systems in place to document employee access to user data. These logs were considered by the DPC in the 2011 Audit Report.

[6] Page 108 of the 2011 Audit Report
[7] Page 108 of the 2011 Audit Report

> *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.* [8]

The DPC also considered the additional safeguards that FB-I deployed to prevent unauthorised staff access 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.*[9]

Following this analysis, the DPC confirmed its satisfaction with the framework in place to restrict employee access to data:

> *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.*[10]

Notwithstanding this finding, the DPC did make two best practice recommendations as to how FB-I could further protect user data.

First, the DPC suggested that there may be scope for FB-I to further enhance its approach to granting access permissions:

> *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.* [11]

The DPC accepted that this issue was already being addressed by FB-I via the creation of a new tool:

> *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.*[12]

Second, the DPC noted a potential challenge with a password reset tool:

> *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.*[13]

In response to this suggestion:

> *FB-I … [undertook] to integrate user password resets by employees into its monitoring tools.*[14]

3.1.6 Screen-scraping

The DPC accepted that FB-I had deployed appropriate safeguards to mitigate the risk of screen-scraping.

[8] Page 109 of the 2011 Audit Report
[9] Page 109 of the 2011 Audit Report
[10] Page 109 of the 2011 Audit Report
[11] Page 109 of the 2011 Audit Report
[12] Page 109 of the 2011 Audit Report
[13] Page 109 of the 2011 Audit Report
[14] Page 109 of the 2011 Audit Report

> *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.*[15]

3.1.7 Documentation

While the DPC was satisfied with the level of security in place by FB-I, it did recommend that further steps could be taken to document its security policy.

> *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.*
>
> …
>
> *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.* [16]

In light of this recommendation, FB-I agreed to further document its approach to security:

> *FB-I will continue to document policies and procedures as required to maintain consistency in security practices.* [17]

3.1.8 Conclusion

Following its far-reaching consideration of FB-I's systems, its testing, its discussions with senior Facebook engineers and the technical report prepared by the DPC's technical expert, the DPC expressed the following view:

> *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.* [18]

3.2 2011 Technical Audit Report

The DPC's findings with respect to FB-I's security, as set out in Section 3.1 of this Response, were based on the 2011 Technical Audit Report which was prepared for the DPC by a member of staff of the University College Dublin Centre for Cybersecurity and Cybercrime investigation. Many of the points made in the 2011 Technical Audit Report were repeated in the 2011 Audit Report and have been set out above.

In addition, the 2011 Technical Audit Report made a number of additional points about FB-I's security.

As alluded to in the 2011 Audit Report, users are provided with a number of optional security features[19], should they wish to avail of them. The 2011 Technical Audit Report took into account those features, including:

> *Secure browsing enables the use of encrypted communication using HTTPS whenever possible.*
>
> …

[15] Page 112 of the 2011 Audit Report
[16] Page 108 of the 2011 Audit Report
[17] Page 109 of the 2011 Audit Report
[18] Page 108 to 109 of the 2011 Audit Report
[19] Page 162 of the 2011 Technical Audit Report

> *Login notifications involves notifying the user whenever their account is accessed from a computer or mobile device that has not been used before.*
>
> …
>
> *Active sessions allows a logged in user to see the locations from which their account is currently logged in and end activity from any particular session if that activity is unrecognised.*
>
> …
>
> *One-time passwords is a feature to allow users protect their account when they log in from a public computer. The user sends an SMS to a particular number and they will receive an eight character temporary password, valid for 20 minutes, which can be used to access their account.*[20]

Attention was also drawn to the protections provided by FB-I in detecting suspicious activity on users' accounts:

> *Facebook also monitor for suspicious activity on user accounts. Detection of suspicious activity will lead to additional authentication steps such as the user needing to fill out a CAPTCHA or by an SMS authorisation code sent to the user's mobile phone.*[21]

The 2011 Technical Audit Report concluded that FB-I's security controls accorded with ISO levels:

> *[I]t has been concluded that Facebook has appropriate information security controls in place, broadly consistent with the requirements of ISO 27001 and 27002.*
>
> *The majority of the controls described by Facebook appear to be effective.*
>
> …
>
> *"If there is a shortcoming in Facebook's information security arrangements it is their informality."*[22]

The matter of corporate security at FB-I was considered in more depth in the 2011 Technical Audit Report. The extent to which employee access to data was logged and analysed was explained by the technical expert:

> *In the particular case of employee access to Facebook user data, Facebook retain a log of every access by every employee of every Facebook user account. This data is examined both automatically to identify patterns of suspicious behaviour and manually when specific cases require investigation. Facebook has demonstrated the functionality of their automated investigative tools. Facebook has also demonstrated that new abuse scenarios are added to the automated investigative tools as they are identified.*[23]

3.3 Update Report

FB-I provided additional information to the DPC in its July 2012 Update Report which is appended to the 2012 Audit Report. This details the enhancements FB-I had implemented regarding employee access to user data since the time of the 2011 audit.

> *There have been no substantial changes to the core Information Security Controls, which were deemed to be adequate during the December 2011 audit by the DPC. However, Facebook was in the processes of making considerable changes to how employee access to user data was managed, which was reviewed in detail in July.*

[20] Page 162 of the 2011 Technical Audit Report
[21] Page 162 of the 2011 Technical Audit Report
[22] Page 163 of the 2011 Technical Audit Report
[23] Page 163 of the 2011 Technical Audit Report

> *Facebook has implemented a permission model that relies on an employee's role in the organization, as dictated by the Human Resources Management system. In addition to changing how permissions are granted and revoked, Facebook spent a significant amount of time building a system that provides granular access to a user's data. Access is granted to a specific employee, for a specific user, within a specific tool, based on a request initiated by the user. The new access method is known as "token based access". Migration to the token-based access is ongoing— at the present time, all inbound requests serviced by operations teams are fully migrated to the token-based access model, and tokens will continue to be implemented across other workflows throughout the next 12 months*
>
> *In addition to the core infrastructure security controls and the new data access controls, Facebook has also made significant progress in their monitoring capabilities. In December, basic data abuse detective capabilities existed and have been further improved to detect new avenues of potential abuse. The biggest change since December is a new a tool Facebook built to detect general security breaches using clustering and anomaly detection across all systems in the infrastructure. This new system goes beyond detecting known types of attacks or abuse, and looks at historical behavior of an account to determine unusual behaviors that could indicate a compromise. This system will continue to be developed, introducing new detection capabilities and operational procedures to respond to potential incidents.*[24]

3.4 2012 Technical Audit Report

3.4.1 Security of User Accounts

The 2012 Technical Audit Report noted that the security features deployed by Facebook to protect user accounts remain in place:

> *"It has been verified that these features [relating to security of user accounts] continue to exist and continue to operate substantially as described in the original technical report."*[25]

The 2012 Technical Audit Report further noted that FB-I had enhanced security for users in the mobile arena by adding encrypted browsing for Android and iPhone users:

> *"The original technical report stated that secure browsing was not supported on the mobile platform. It has been confirmed as part of the current testing that communication is encrypted using TLS' (version 1.2) between Facebook and both the iPhone and Android Facebook applications. TLS version 1.2 is an industry standard encryption algorithm and is believed to offer adequate security."*[26]

3.4.2 Corporate Information Security

The 2012 Technical Audit Report contains an intensive and highly detailed examination of the security of FB-I's corporate information security systems. This is set out, for reference, in full below:

> *In the previous audit an attempt was made to gain an overall understanding of information security controls in place within FB-I. At that time it was further concluded that the majority of the controls described by FB-I appeared to be operating effectively. Information security controls within FB-I have not substantially changed in the intervening months and it is therefore concluded that FB-I continue to maintain and adequate information security stance.*
>
> *It was noted at the time of the previous audit that FB-I expend considerable effort to manage employee access to user data. This second review has been used as an opportunity to study this matter in considerable detail. The results of this examination can be found in the following sections.*
>
> *Access to user data is controlled by permissions assigned through an internal permission management system. This permission management system uses a variation on a standard "user, role, permission" logical access control model. Access*

[24] Page 63 of the Update Report

[25] Page 10 of the 2012 Technical Report

[26] Page 11 of the 2012 Technical Report

permissions are divided into broad categories known as domains. To a first approximation, domains can be thought of as roughly equivalent to individual internal tools[27]. Within a domain is a set of actions that can be carried out within the context of that domain. These actions are analogous to permissions[28]. The ability to perform any particular action can be assigned to an individual employee more commonly to a role. Employees can be assigned to these roles, which contain sets of permissions appropriate to a function within the organisation.

1.3.2.1 Account Provisioning

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

1.3.2.2 Granting Permissions

Permissions can be granted to employees in several ways:

Roles can be configured to match patterns of employee information within the organisational database. An employee that matches such a pattern will therefore be automatically granted this role. These roles are defined in terms of parameters such as the employee's geographical location or job title. It is notable that if the employee's role changes in the human resource management system, this will automatically propagate to the organisational database and their account will therefore automatically be removed from any roles that are no longer relevant to their new position. No administrative action is required in these cases.

- *An employee can also be manually added to a role or granted a specific action by an administrator based on an ad-hoc request. These requests are circulated by email to a per-domain list of approvers, which consist of the owners of the domain and also information security staff.*
- *Software engineers can self-grant themselves temporary access to a certain domain. This is predominantly used for bug fixing. A notification email is sent to the domain administrators when such temporary access has been granted and the permissions are automatically revoked after 14 days. This self -granting of permissions is only possible by software engineers.*

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

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

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

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

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

[28] The terms "permissions" and "actions" are used interchangeably below.

The list of access requests for a sample 30 day period were reviewed to determine what proportion of requests are approved by the domain owners and what proportion are approved by information security. In the period examined, 46.54% of the access requests received were approved by information security.

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

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

- *Typically in response to a report of a bug, an engineer visits a tool and attempts to perform an action for which they do not have permission.*
- *The engineer receives a permission denied screen that contains a "Get Permission Now" button.*
- *When the "Get Permission Now" button is clicked, the engineer fills in the reason why they need the access.*
- *On the same screen, prior to submitting the request for the permission, the engineer is warned to be careful and a reference to the acceptable usage policy is included on the screen*[29]*.*
- *The engineer is then granted permission to access the tool for two weeks.*
- *When engineers grant themselves permission to a tool in this way, an email is received by the domain owners stating that the engineers have granted themselves permission to the tool. This email contains the reason provided by the engineer as to why they needed access and also contains a link to FB-I's internal CERT (Computer Emergency Response Team) where the domain owner can report inappropriate access by an engineer. FB-I report that such administrative reports are rare.*

1.3.2.3 Revocation of Permissions

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

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

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

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

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

- *If an employee moves role;*
- *Permissions automatically granted based on the employee's old role will be automatically revoked.*
- *Any unused permissions will be automatically revoked after 45 days.*
- *The employee is sent an email and asked to confirm if they still need any remaining roles or permissions.*

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

- *If an employee leaves the organisation, all of their permissions are automatically revoked upon removal of their record from the human resource management system.*

1.3.2.4 Logging of Permission Usage Activity

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

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

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

1.3.2.5 Token-based Access Model

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

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

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

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

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

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

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

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

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

1.3.2.6 Administrative Privileges

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

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

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

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

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

1.3.2.7 Abuse Detection

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

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

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

- *Numerous failed attempts to use a particular permission, followed by successful use of that permission.*
- *A relationship between an employee and the data they are accessing. For example, an employee accessing their wife's data.*
- *Access to sensitive user accounts (e.g. celebrities).*
- *Deviations from a normal usage pattern. For example, an employee accessing a disproportionate number of female user accounts when a typical access pattern for an individual in a similar role is 50% male, 50% female.*
- *Issuing refunds to a user with whom the employee has a relationship.*

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

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

> *employees in the same department and the usage pattern of all employees in the organisation.*
>
> *These reports are also generated once per week and are sent to the two independent security teams for review.*
>
> *Evidence of the delivery of automated email reports to security teams has been provided.*
>
> *If a security team member, while examining one of the reports, believes that an abuse incident has taken place, they escalate the matter to HR and legal for further review and action. Facebook supply documented guidance to the security team to assist team in determining whether a particular incident constitutes abuse. The guidance documentation has been reviewed and confirmed to provide guidance consistent with the representative list of suspicious activities listed above.*
>
> *Facebook have a further control in place to prevent employees covertly accessing other employee's accounts; If employee A accesses employee B in the user admin tool, employee B will receive an email notification stating that employee A has accessed their data. If this access is not authorised, employee B can raise an incident with the security team, which will be handled as described above. A legitimate use-case for employees accessing each other's accounts would be if a software engineer needed access to an employee's account to resolve a reported bug.*
>
> *Finally, Facebook have also deployed a network intrusion detection system to detect anomalous behaviour that may indicate a data breach or attempted data breach.*
>
> *1.3.2.8 Sample Permissions Review*
>
> *A random sample of employees was selected and the permissions granted to those employees were reviewed to determine whether they were appropriate for the roles of the individuals within the organisation.*
>
> *The permissions of the employees and the level of access to user data were consistent with, and not excessive for, the roles of the selected individuals.*[30]

3.4.3 Scraping

The DPC's technical expert further considered the steps that FB-I had taken to prevent the "scraping" of profiles. Having previously looked at this issue in 2011 Technical Audit Report, the technical expert noted his continued satisfaction with FB-I's approach to this issue:

> *Scraping, also known as screen scraping, is the name given to an automated process of harvesting data from a website. In the case of Facebook, the concern surrounds the ability of an automated process to gather a large volume of information about Facebook users.*
>
> *As part of the previous review, FB-I provided details of the arrangements they have made to prevent scraping. It was concluded that the arrangements adequately mitigate the risk of largescale harvesting of Facebook user data while allowing service to be effectively provided to legitimate users in a wide range of circumstances.*
>
> *Facebook have confirmed that the arrangements to prevent scraping are still in place and have not changed since the last review.*[31]

[30] Pages 11 to 18 of the 2012 Technical Audit Report

[31] Pages 40 to 41 of the 2012 Technical Audit Report

3.5 2012 Audit Report

In the 2012 Audit Report, the DPC stated that "*significant time on the re-audit was focused on assessing FB-I's approach to data security*".[32] This assessment was set out in the 2012 Technical Audit Report.

At page 40 of the 2012 Audit Report, the DPC noted there had been a satisfactory response by FB-I to the best practice recommendations contained in the 2011 Audit Report. The DPC also noted its continuing satisfaction with other aspects of FB-I's security.

> ***Recommendation: Many policies and procedures that are in operation are not formally documented. This should be remedied.***
>
> *FB-I supplied a number of polices in relation to internal access to personal data and the procedures and practices in place for granting and removing such access as well as ensuring that all such access when granted is appropriate.*
>
> ***Recommendation: We are satisfied that FB-I does have in place an appropriate framework to ensure that all access to user data is on a need to know basis. However, we recommended that FB-I expand its monitoring to ensure that there can be no employee abuse through inappropriate password resets of a user's account***
>
> *FB-I implemented this recommendation during January 2012*
>
> ***Recommendation: We were concerned that the tools in place for ensuring that staff were authorised to only access user data on a strictly necessary basis were not as role specific as we would have wished***
>
> *FB-I has enhanced its tools and procedures in this area to a level that is acceptable to this Office. It has in place strict approvals for employee access to particular tools, peer review of such approvals and the withdrawal of such access after a specified period or where no actual use of the access provided has taken place. This is supplemented by extensive logging and monitoring of employee access which is constantly refined to ensure that, in so far as is possible, that patterns of inappropriate access are detected. This Office is therefore satisfied that FB-I has in place an appropriate framework for ensuring that access to user data is strictly controlled and monitored.*
>
> *We note that FB-I is in the process of further enhancing its approach in this area by moving to a model of approved access to specific user accounts in response to specific issues arising. This should further assist to restrict the potential for inappropriate access to user data on the site.*
>
> …
>
> ***December Audit Conclusion: We believe that current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data via "screen scraping" while allowing the service to be effectively provided to legitimate users.***
>
> *The position on this issue is unchanged.*[33]

4 APPLICATION TO CURRENT COMPLAINT

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

(a) *"Facebook Ireland only seems to be encrypting passwords and credit card numbers."*

As can be seen from the URLs included in the Complainant's Request for Formal Decision, any user can enable encrypted (https) Facebook browsing. This feature was noted in the DPC's 2011 Audit Report, as

[32] Page 39 of the 2012 Audit Report

[33] Page 40 of the 2012 Audit Report

set out in Section 3.1.3 above. As noted in Section 3.4.1 of this Response and in the 2012 Technical Audit Report, encrypted browsing now extends to encrypted browsing for mobile users.

(b) *Statements in Facebook's terms and privacy policy "make it very questionable if Facebook Ireland is seriously protecting personal information. In fact, they are not even claiming that they are protecting it; they are straight out saying that they do not guarantee any security."*

Having extensively reviewed FB-I's systems, practices and policies throughout the audit process, the DPC has expressed the view that FB-I deploys appropriate security to protect user data. As mentioned in the previous paragraphs the DPC explicitly stated in its 2011 Technical Audit Report that FB-I's security controls were equivalent to the industry leading ISO 27001 and ISO 27002 security standards.

(c) *"even the most basic [app developer] provisions (such as providing some kind of privacy policy) are … not enforced by Facebook Ireland."*

This issue is addressed in our Response to Complaint 13 – Apps, where it was noted that FB-I developed an automated tool to check that apps have a live link to a privacy policy.

(d) *Facebook is failing to take appropriate steps to secure applications.*

FB-I deploys considerable technical and organisational resources to endeavour to make the Facebook platform safe for its users. This issue is addressed at length in our Response to Complaint 13 – Apps.

(e) *Facebook is failing to take appropriate steps to prevent the scraping of user data*

As the DPC confirmed in the 2011 and 2012 Audit Reports and the 2012 Technical Audit Report, the *"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."*[34]

(f) *That 2011 Audit Reports suggest that FB-I acted unlawfully by not having appropriate security in place*

FB-I strongly rejects this unfounded implication.

The Complainant assumes that by virtue of the DPC providing best practice recommendations in the 2011 Audit, this has somehow translated to an implication of unlawfulness. FB-I refutes this mischaracterisation and would note the following from the Executive Summary of the 2011 Audit 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.*[35]

Furthermore, as noted above, the 2011 Technical Audit Report found that FB-I's security controls were equivalent to ISO 27001 and ISO 27002. In addition, while the DPC did make best practice recommendations to enhance FB-I's security, it was:

> *[S]atisfied 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.*[36]

(g) *The audit "in no way tested or reviewed the proper functioning or even the existence of the controls"* [37] and has not "*established any verifiable facts concerning this matter. It has merely relied on hearsay and absurd arguments*"

[34] Page 111 of the 2011 Audit Report and page 40 of the 2012 Audit Report
[35] Page 4 of the 2011 Audit Report
[36] Page 109 of the 2011 Audit Report
[37] Page 118 of the Request for Formal Decision

This statement is unfounded. As can be seen from Section 3 of this Response, the DPC and its external technical expert conducted an in-depth, far-reaching and extensive review of FB-I's security practices.

(h) The capabilities of the DPC's external expert are "questionable".

We note that the DPC was assisted in the audit by Mr David O'Reilly of the University College Dublin Centre for Cybersecurity and Cybercrime investigations. It is a matter of public record that Mr O'Reilly specialises in cybercrime and computer forensics. FB-I had sufficient confidence in Mr O'Reilly's skill and expertise to grant him access to Facebook's technological stack and code base.

(i) "There was no proper limitation of access within the company on a 'need to know' basis."

This statement is incorrect and diametrically opposed to the DPC's finding 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.*[38]

[38] Page 109 of the 2011 Audit Report