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

Response to Complaint(s) Number: 7

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 7 – MESSAGES

1. BACKGROUND

1.1 What are Facebook messages?

FB-I offers its users an integrated messaging service. This service allows users to chat (like traditional instant messaging), send longer messages to other Facebook users and send and receive emails to and from non-Facebook email addresses.

In offering this service, FB-I acts as an intermediary, facilitating communication amongst users and between our users and non-users. Where user A sends a message to user B, copies of this message will appear in both user A's and user B's inboxes; FB-I stores this message on behalf of *both* user A and user B.

1.2 Data Use Policy

In the Data Use Policy, FB-I informs its users that FB-I may receive and process their personal data as a result of their use of messages. FB-I also informs its users that messages may be retained until the last user has deleted the message:

> *We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook.*
>
> …
> *Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.*

1.3 Help Center

FB-I also provides extensive information about how messaging works in the Help Center.

2. FACTUAL ASSERTIONS MADE BY COMPLAINANT

The Complainant objects to the manner in which Facebook messages work. In the Original Complaint, the Complainant alleges the following, which is reiterated in the Request for Formal Decision:

(a) *"When users 'delete' messages, they are only tagged as deleted and the user cannot see them anymore, while Facebook Ireland is actually still holding them on its system."*

In the Request for Formal Decision[1], the Complainant further alleges that:

(b) *"FB-I is capable of retrieving all deleted messages of a particular users, even when he/she deleted at the copies that were stored in the original section of the system."*

(c) *"He cannot see any facts or material arguments that would support the claim" that "messages are fully deleted when all data subjects that have been part of the conversation have deleted the message."*

(d) *"There is no fact based evidence of the extent of processing of the content of messages."*

[1] Pages 67 to 68 of the Request for Formal Decision

(e) *"FB-I generates endless amounts of personal, private chat messages that can factually not be deleted".*

(f) *It is practically impossible for users to delete all their messages with reasonable efforts.*

(g) *"FB-I is legally obliged to disclose the users' information upon orders by authorities from all over the EU or the US. In addition FB-I also allows authorities of other countries to get copies of this highly personal communication….This issue has become especially obvious after the revelations around the 'PRISM' project, which allows for direct access to the servers of FB-I. Through such systems the authorities can access factually every chat message that any user of facebook.com has sent or received ever since facebook.com was launched".*

(h) *"FB-I also has a factual monopoly on instant messaging (IM) which means that most data subjects have no possibility to avoid this system".*

3. AUDIT PROCESS

3.1 Introduction

FB-I's approach to messages was subject to extensive scrutiny during the DPC's audit. Arising out of this process, FB-I made a number of modifications to its policies with respect to messages and gave its users further control over the retention of such communications.

During the audit, the DPC addressed three separate issues in connection with messages.

First, the DPC considered FB-I's policy of retaining a copy of a message until all parties to a communication had deleted that message.

Second, the DPC investigated the purposes for which messages were processed.

Third, the DPC explored whether FB-I could enhance the information it provided to users in connection with the retention of messages.

3.2 Retention of Messages

During the audit, the DPC considered, on a technical and policy level, FB-I's approach to retaining messages. These investigations confirmed that FB-I retains messages until the parties to that message have deleted it from their inboxes. The 2011 Audit Report further accepted that Facebook's approach in this respect is in line with best practices.

3.2.1 2011 Audit Report

In the 2011 Audit Report, the DPC set out its understanding of the Complainant's allegations:

> *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.* [2]

[2] Page 73 of the 2011 Audit Report

These allegations were subject to a preliminary technical review during the 2011 audit. The conclusions of this analysis were set out in the 2011 Technical Audit Report:

> *Message deletion is performed based on reference counting*[3]*. This means that when the last user who had a copy of the message deletes the message, that message will be permanently deleted… It has not been possible to positively confirm that messages are deleted when the reference count drops to zero.*[4]

Based on these initial technical findings, and noting that further testing would be required, the DPC considered FB-I's policy of retaining a copy of a message until it had been deleted by all relevant users and accepted that, due to Facebook's position as an intermediary, this policy was in line with best practices:

> *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.*[5]

This policy of retaining a copy of a message until all parties to the message have deleted it was separately acknowledged in the deletion section of the 2011 Audit Report:

> *At the present moment, while most shared content is deleted when one party deletes it, some shared content … in the case of Messages, is not deleted until all parties have deleted the content*[6]

3.2.2 Update Report

FB-I's Update Report provided a detailed technical description of FB-I's retention policies with respect to messages.

> *5.2 Deletion of Messages*
>
> *FB-I enables messages to be sent directly from one user to one or more other specified users. In these instances, the sender and each recipient can access a copy of the message in his or her account, and FB-I retains a copy of that message in order to permit this access. In the Report of Audit, the DPC expressed that FB-I's policy and practice to delete a message entirely after all parties to the communication have deleted their copies of the message was an acceptable approach. The DPC indicated that this approach would be confirmed during the July review.*[7]
>
> …
>
> *11.2 Other data stores*
>
> *FB-I operates a few other specialised backend data stores. The two most interesting such stores are Titan, which is built on HBase and stores private messages, and Haystack, which is a custom space-efficient large-blob store used to store photos and private message attachments.*
>
> *It's important that these data stores have the same properties of reliable deletion and rapid recovery from unintended deletions when discovered quickly. In both cases, this is implemented by flagging a record as deleted so that it is hidden from the site immediately, then purging the deleted data periodically. To further ensure our ability to recover photos that were unintentionally deleted, the first compaction over an object does not actually purge it unless sufficient time has passed. In no case, however, does this process take more than 90 days to completely*

[3] *Reference counting is a technique of storing the number of references to a resource and using this reference count to deallocate objects that are no longer required.*

[4] Page 195 of the 2011 Audit Report

[5] Page 73 of the 2011 Audit Report

[6] Page 116 of the 2011 Audit Report

[7] Page 40 of the Update Report

> *purge the data.*
>
> *Titan's use of shared message attachments is the last area of special requirements. When a user sends a private message to a friend on Facebook, each user ends up with an independent copy of the message body except any attachments. The attachment is actually stored in Haystack as a binary large object. Unlike the user databases where traditionally relational database features are available (e.g., transactions and locks), each HBase cell in Titan is completely independent. This makes a reference counting implementation far more complicated and error-prone. Thus we take a simpler approach. Each attachment is encrypted with a unique per-message, per-attachment key. This key is only stored in the sender's and each recipient's copy of the message. As each user deletes their copy of the message, they delete their copy of the encryption key. Once the last remaining user deletes their copy, FB-I is no longer able to decrypt the stored attachment. The encrypted attachment's metadata does not include any information about the sender or the recipients of the attachment. This results in some storage inefficiency (these attachments could otherwise be deleted to free space), but the benefits in reduced complexity and increased reliability are far more important. If the storage later becomes a problem, we will likely be able to identify orphaned encrypted attachments and delete even the encrypted data.*[8]

3.2.3 2012 Technical Audit Report

Following an extensive technical examination of FB-I's systems and code base, the 2012 Technical Audit Report set out the following account of Facebook's storage of messages:

> *1.9.2.4 Titan Data*
> *Titan is the name of the Facebook private message storage area. Interactions with the titan storage area can take place via the Facebook website, for example via interactive chat and via Facebook email. Incoming emails for Facebook users are also stored in Titan.*
>
> *Messages are stored in Titan using HBase. The architecture of HBase consists of a number of cells, with a fraction of users allocated to each cell. There is no association between the data stored in separate cells. To clarify this point, consider the case of user Alice sending an email to user Bob where Alice's messages are stored in cell A and Bob's messages are stored in cell B. When Alice sends the message to Bob, the copy of the message stored in her 'Sent' messages will be stored in cell A and the copy of the message stored in Bob's 'Inbox" will be stored in cell B. The point being that two copies of the message are stored, one in Alice's cell and one in Bob's cell.*
>
> *If Alice subsequently deletes her account, the copies of all of her messages are deleted from Titan. Bob's copy of the email will not be deleted when Alice deletes her account. This is as one would expect with an email service.*
>
> *Titan also supports message attachments but they are handled differently. The message itself is stored in Titan but the attachment itself is stored in haystack (see Section 1.9.2.3) with a reference to the haystack location stored in Titan along with the message.*
>
> *Since there is no association between cells, the problem that now arises, within the context of account deletion, is how to know when the last reference to the attachment has been deleted, and therefore whether to delete the attachment. Using the example above; when Alice deletes her account, if Bob has a copy of a message with an attachment from Alice it would not be appropriate to delete the attachment when Alice deletes her account because that would delete Bob's copy.*
>
> *Centralised reference counting is a possibility but that option was dismissed by FB-I as being too operationally unreliable in practice, considering the particular quirks of the technologies in question. Another alternative would be to scan all other cells in Titan to determine whether any other references to the attachment are left. This would remove the advantage of the fact that there is no association between cells.*
>
> *Therefore, the solution that has been implemented is that when the attachment is being stored in haystack, it is encrypted using 256-bit AES and a copy of the key is stored with each copy of the message. This means that when the last copy of the message is deleted there is no way for anyone to retrieve the content of the attachment*

[8] Pages 66 to 67 of the Update Report

> *because all copies of the decryption key have been deleted. At the present moment, this system means that the space in haystack is permanently leaked.*[9]

3.2.4 2012 Audit Report

In its 2012 Audit Report, the DPC confirmed that this issue had been resolved to its satisfaction and closed out on this issue by simply noting that:

> *We … confirmed that in a situation where both the sender and recipient of a message or chat on the site deletes an individual message that it is not retained in any form and is deleted in line with the process outlined in the Technical Analysis Report.*[10]

3.2.5 Retention: Conclusion

FB-I only retains messages until they have been deleted by the sender and the recipient. This state of affairs, which was confirmed to the DPC's satisfaction following extensive technical examination, continues to this day.

3.3 Scanning of Messages

FB-I primarily processes messages to provide its users with the communication service they requested. Facebook also scans messages to a limited extent for child protection purposes. This position was considered by the DPC during the audit process.

3.3.1 2011 Audit Report

In the 2011 Audit Report, the DPC acknowledged FB-I's confirmation that it does not use content of messages/chat for advertising targeting purposes.[11]

3.3.2 2012 Technical Audit Report

This issue was considered in further depth in the 2012 Technical Audit Report. The results of the technical investigation into this issue were set out in the following terms:

> *2.4 Private Message Content*
>
> *As part of this audit, Facebook were asked to provide information about what, if any scanning (aside from anti-virus and anti-spam scanning) is performed on user's private message content.*
>
> *It has been reported in the media that Facebook scan private messages in an attempt to identify child predators. Facebook have confirmed, as part of this audit, that scanning of a tiny fraction of private messages is taking place and have provided a description of the scanning process as follows; queries based on what FB-I describe as "objective non-content criteria determined to provide reasonable detection of a violation of certain terms of use of the service" identify a very tiny slice of sender-recipient pairs that match a specific profile. Stored messages matching that profile are ranked based on a specific list of keywords and a small number of the highest ranking conversations suggesting a possible risk of imminent harm are then queued for human review by a team of experts.*
>
> *A full, detailed review of the operation of the private messaging system is beyond the scope of this audit.*[12]

[9] Pages 50 to 51 of the 2012 Technical Audit Report
[10] Page 23 of the 2012 Audit Report
[11] Page 46 of the 2011 Audit Report
[12] Page 54 of the 2012 Technical Audit Report

3.3.3 2012 Audit Report

In light of the 2012 Technical Audit Report, and the DPC's broader investigation into Facebook's operations, the DPC accepted FB-I's position that it did not use the content of messages for advertising purposes:

> *FB-I has clarified that it does not conduct ad-targeting based on the content of messages and chat on the site. This Office sought to conduct a technical analysis to confirm this was the case by assessing all scans sent to messages on the site. This task while technically feasible was ultimately not undertaken at this point due to time constraints during the process. As it happens, during the course of the audit a concern arose from comment in the media as to scanning of messages that was taking place for what was stated to be the prevention of crime. While this has transpired to be focused solely on the prevention of child sexual grooming, this is nevertheless an area on which this Office will need to work with FB-I to ensure that all such scanning takes place taking full account of data protection requirements. This engagement will provide the context in which a definitive examination of the use of content from messages and chat will take place.*[13]

3.3.4 Scanning of Messages – Conclusion

As the DPC noted, FB-I engages in a limited scanning of messages for security reasons, notably the prevention of child abuse. Facebook does not scan messages for other purposes, such as advertising.

3.4 User Information

During the audit, the DPC recommended that FB-I further enhance its explanation of its retention policies around, among other things, messages. The recommended refinements were made to the DPC's satisfaction.

3.4.1 2011 Audit Report

In the 2011 Audit Report, the DPC accepted that FB-I's approach to retaining message information was in line with best practice (see Section 3.2.1 above). However, the DPC recommended that FB-I could enhance its disclosures around such retention:

> *At present, the information provided to users in relation to what actually happens to deleted or removed content, such as … messages could be improved. This is accepted by FB-I and will be reflected in an updated Data Use Policy.*[14]

3.4.2 2012 Audit Report

In the 2012 Audit Report, the DPC noted that it was satisfied with FB-I's response to its suggestion that users be provided with improved information in relation to removed messages. As noted above, the Data Use Policy currently provides:

> *Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.*

4. APPLICATION TO CURRENT COMPLAINT

In light of the above, FB-I responds to the Complainant's specific factual allegations as follows:

(a) *"When users 'delete' messages, they are only tagged as deleted and the user cannot see them anymore, while Facebook Ireland is actually still holding them on its system."*

[13] Page 18 of the 2012 Audit Report
[14] Page 71 of the 2011 Audit Report

This is untrue. The DPC has confirmed, following extensive technical investigation, that messages are deleted when the last party to the communication deletes them.

(b) *"FB-I is capable of retrieving all deleted messages of a particular users, even when he/she deleted at the copies that were stored in the original section of the system."*

This is untrue. Following extensive technical examination, the DPC found that when a message is sent across Facebook two copies of that message are stored: one copy associated with the sender and one copy associated with the recipient. When a user closes their account, or deletes a message, their copy of the message is deleted. Messages to or from a user stored in *other users'* mailboxes cannot be retrieved by Facebook when searching against that user.

The Complainant's position amounts to little more than an assertion that, as the 2012 Technical Audit Report disagrees with his views, it must be "*absolutely false*".

(c) *"[H]e cannot see any facts or material arguments that would support the claim … that messages are fully deleted when all data subjects that have been part of the conversation have deleted the message.* [15]

As noted in Section 3.2.4 of this Response, the DPC confirmed during the second technical audit that messages are fully deleted when all users have deleted the message.

(d) *"There is no fact based evidence of the extent of processing of the content of messages."*

As is noted in Section 3.3 of this Response, the DPC considered the "*extent of processing of the content of messages*" during the second audit.

(e) *"FB-I generates endless amounts of personal, private chat messages that can factually not be deleted."*

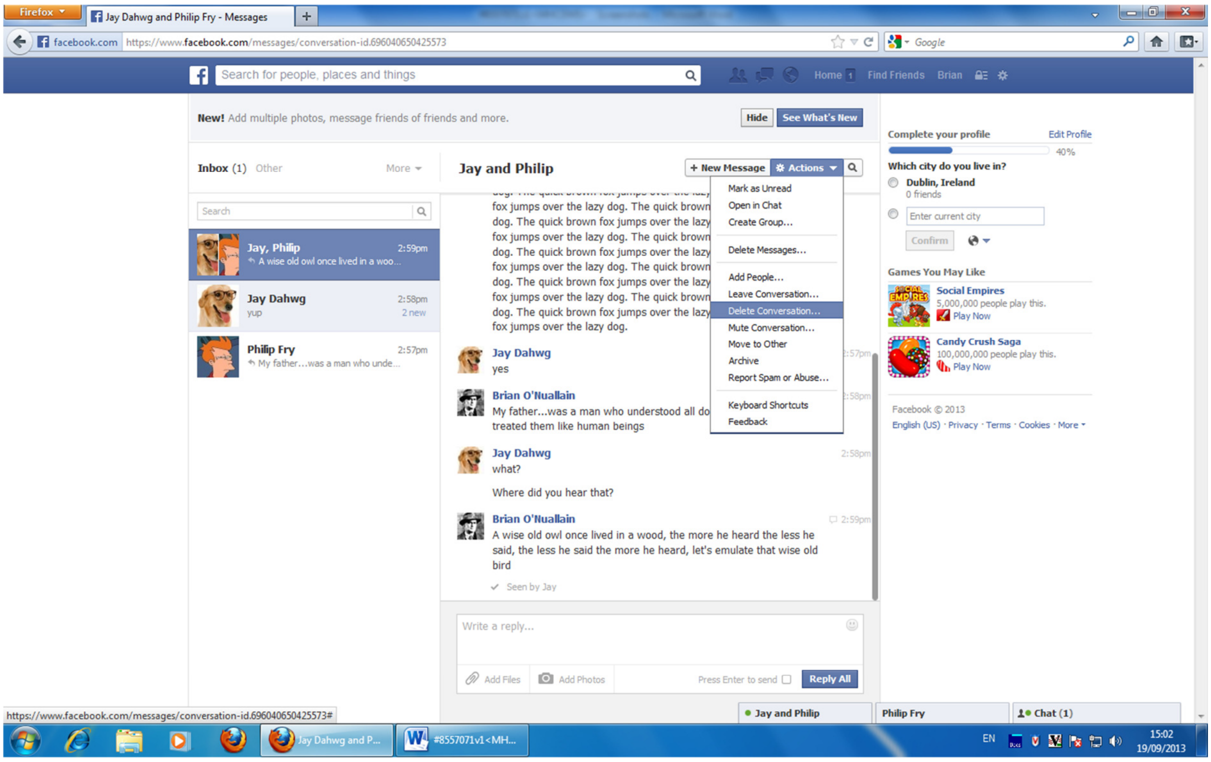
Users may utilise Facebook's free private messaging service to communicate and converse with each other. FB-I does not generate any personal, private chat messages. To say messages cannot factually be deleted is simply incorrect. As is noted in Section 3.2.4 of this Response, the DPC confirmed during the second technical audit that messages are fully deleted when all users have deleted the message.

(f) *It is practically impossible for users to delete all their messages with reasonable efforts.* [16]

The Complainant asserts that for a user to delete copies of all their conversations "*would take hours*". This is simply untrue. FB-I provides a dropdown menu in each conversation allowing users to, among other things, delete specific messages or the entire conversation. It is a relatively easy and straightforward task for a user to delete a message, as can be seen from the screenshot below:

[15] Page 67 of the Request for Formal Decision

[16] Page 69 of the Request for Formal Decision



New! Add multiple photos, message friends of friends and more.

Jay, Philip 2:59pm
A wise old owl once lived in a woo…

Jay Dahwg 2:58pm
yup 2 new

Philip Fry 2:57pm
My father…was a man who unde…

Jay and Philip

fox jumps over the lazy dog. The quick brown
dog. The quick brown fox jumps over the lazy
fox jumps over the lazy dog. The quick brown
dog. The quick brown fox jumps over the lazy
fox jumps over the lazy dog. The quick brown
dog. The quick brown fox jumps over the lazy
fox jumps over the lazy dog. The quick brown
dog. The quick brown fox jumps over the lazy
fox jumps over the lazy dog.

Jay Dahwg 2:57pm
yes

Brian O'Nuallain 2:58pm
My father…was a man who understood all do
treated them like human beings

Jay Dahwg 2:58pm
what?

Where did you hear that?

Brian O'Nuallain 2:59pm
A wise old owl once lived in a wood, the more he heard the less he said, the less he said the more he heard, let's emulate that wise old bird

Seen by Jay

Complete your profile Edit Profile
40%

Which city do you live in?
○ Dublin, Ireland
0 friends
○ Enter current city

Games You May Like

Social Empires
5,000,000 people play this.

Candy Crush Saga
100,000,000 people play this.

Facebook © 2013
English (US) · Privacy · Terms · Cookies · More

(g) *"FB-I is legally obliged to disclose the users' information upon orders by authorities from all over the EU or the US. In addition FB-I also allows authorities of other countries to get copies of this highly personal communication….This issue has become especially obvious after the revelations around the 'PRISM' project, which allows for direct access to the servers of FB-I. Through such systems the authorities can access factually every chat message that any user of facebook.com has sent or received ever since facebook.com was launched".*

These are new claims in the context of messages, but this issue was separately addressed at length during the audit. FB-I's approach to governmental requests is set out in the 2011 Audit Report. The Complainant has filed a separate complaint in connection to the alleged "Prism" program so these issues appear to be best dealt with in the context of this separate complaint. However, for the sake of absolute clarity, we would take this opportunity to again reiterate Facebook's position on this issue: Facebook is not and has never been part of any program to give the US or any other government direct access to our servers. We have never received a blanket request or court order from any government agency asking for information or metadata in bulk. If we did receive such a request, we would fight it aggressively.

(h) *"FB-I also has a factual monopoly on instant messaging (IM) which means that most data subjects have no possibility to avoid this system."*[17]

Again, this is a new allegation in the context of messages, but was previously made by the Complainant in the context of consent.

All persons are free to decide whether or not they wish to use Facebook as a method of communication and social networking. Facebook is only one of many popular forms of communication, including a number of popular instant messaging services, which people utilise today. Facebook does not currently hold a factual monopoly on instant messaging.

[17] Page 72 of the Request for Formal Decision