Summary of Arguments

Meeting of „europe-v-facebook.org" and Facebook Representatives
DATE: February 6th 2012, LOCATION: NH Hotel, Airport, Vienna, AUSTRIA

Concerning the 22 complaints we (europe-v-facebook.org) filed against Facebook Ireland Ltd. we engaged in a meeting with two representatives of Facebook in Vienna. In order to ensure the maximal possible transparency we tried to have a transparent protocol about the arguments that were exchanged between the two parties.

We decided to list the arguments in the order of the 22 complaints to enable readers to get a well-structured summary of the discussion. While most of the arguments are presented in a summarized way, we decided to quote certain crucial arguments in the exact wording used by Richard Allan (Director of Policy, FB Ireland) or the member of the "Policy Team" of FB USA. Since this member was so far not a publicly known figure we did not disclose her name.

We gave Facebook the possibility to comment on this summary before publication to avoid obvious mistakes or misunderstandings, but this is *not* a joint statement. The comments were given by Richard Allan (Director of Policy, FB Ireland). Whenever we thought the implementation of a comment by Facebook was impossible because it was neither matching our protocol nor our memory of the meeting we decided to put the comment in a footnote. Facebook's comments that were, to our understanding, simply using another wording were not implemented in the document.

We hope this Summary of Arguments will enable everybody to get a clear picture of the arguments and counterarguments of the two parties. Even though we would have wished for more transparency, we believe that this document makes the negotiations more transparent than most other proceedings around Facebook.

europe-v-facebook.org

Who is the "Controller"? *As most legal systems data protection law has to clarify who is responsible for a specific act.*	**europe-v-facebook.org** - There has to be a clear decision on the controller issue. When this is not clear by the facts, there has to be a contractual clarification. This is the basis for all other legal examinations. - We think the user is the controller of what we called the "first basket" (e.g. the wall/timeline, pictures uploads, events…); This is in line with the "Lindqvist" case decided by the ECoJ and supported by the fact that the user decides on the data process; - For this "first basket" Facebook is the mere host and may be obliged to e.g. take down illegal content just like any other host provider. - Facebook would have to follow the obligations as a mere processor (*see complaint 18*) and give users sufficient options to fully control the all data that falls under this "first basket". - In a second step Facebook is gets the right to use this hosted data from the "first basket" for its own purposes "second basket" by obtaining consent from the data subject (e.g. aggregating the news feed, friend suggestions, advertisement…) - The fact that Facebook designed the platform does not mean it is the controller for all processing; The designers of HTML are as well not the controllers of all HTML pages;	**Facebook** **-** Legislation was not designed for social media, therefore FB does not have a general statement on who the controller is - The "two basket" idea does not work for Facebook - If FB would shift responsibilities to the user this would be seen as trying to avoid responsibility by data protection authorities and the public / media - FB feels it has to be the controller of most processing in order to allow FB to intervene whenever necessary (e.g. takedowns)[1] - Because FB-I has to take down inappropriate content, it has to be the controller and is "far beyond the mere host"[2] - Richard: "We are the controller for what we control"; "The user has some responsibility too" - FB Ireland is the controller for facebook.com outside of the US and Canada[3] *[1] changed to: "…to carry out a range of functions as set our in the data user policy"* *[2] Statement fully deleted in FB's comments* *[3] FB added two statements:* *" - FB explained that it is clear from the structure of the site and the data use policy that it is not following the model described by europe-v-facebook"* *" - FB sees no reason for there to be a single model for the data user policies of a social network"* - FB is controlling the functionalities of the page, which makes it the controller
Definition of a valid "Consent"? *FB claims that all processing is based on the users' "consent". Consent in data protection law is a very high bar to meet.*	**europe-v-facebook.org** - We believe that Facebook has to stick to the legal definition of a consent (see Irish DPA and Directive 95/46/EG) - This means that the consent has to be (1) *unambiguous*, (2) *freely given*, (3) *specific*, (4) *informed* and (5) *not obtained by deception or misrepresentation (see D. Kelleher, p. 209)*	**Facebook** - We got consent to everything through the privacy policy and all amendments to it **-** No one needs to post something **-** Richard „Most of what we do needs a new definition of consent"; "If the user is surprised we have to make it more comprehensive"; - K***: "Cannot speak for FB as a whole"; "We have to look at the clarity of the language"; "Your complaints raised a lot of good issues" *<u>Note:</u> We repeatedly asked for a clear answer to our question*

01 Pokes	**europe-v-facebook.org** **-** We think "pokes" fall under the "two basket" principle just like an e-mail that is processed for secondary purpose by a provider. **-** There is no information on the secondary purposes for which the "pokes" are processed besides the mere "poke". **-** Since the <u>recipient</u> is the one deleting the "poke", it is not stringent that all pokes are kept for indefinite time for rare cases of cyber bullying. - It's the recipient's decision to either keep or delete it. If the recipient feels that the poke should be kept for one or the other purpose (e.g. as evidence) the recipient can choose to do so - If Facebook has compelling reasons that make retention necessary, there has to be a deletion routine after a certain time; We suggest that there should be certain standard time periods for all data categories so that users can understand it better; - There is currently no information to the users that pokes are retained for an indefinite time.	**Facebook** - Old "pokes" are kept for the case of cyber bullying and other similar cases (K***: "All sorts of reasons"); The exact other purposes for which old "poke" information is used is not known; - FB has not yet decided on a time after which old "pokes" are automatically deleted; They will not be kept longer than necessary; - There will be a possibility to actively delete old pokes in the „activity log" - There will be a "much clearer" retention policy - Changes are scheduled for the next couple of weeks <u>Follow up:</u> - For which purposes is the "poke" information used? - For how long will "deleted" pokes be kept by FB?
02 Shadow Profiles	**europe-v-facebook.org** - Imported address books fall under the "first basket" and generally fall under the "household exemption" since they are not processed by or displayed to anyone but the user that imported them. Facebook is the mere host / processor. - We think that an invitation that is sent by a Facebook user to friends is just like a usual e-mail and falls under the "household exemption" as long as Facebook is only processing it.	**Facebook** **-** The user is the sole controller of imported contact details and falls under the "household exception" - Facebook is only the processor for imported contact details and does not use them in any way, unless the user is actively using them for "friend finder" purposes - When a user invites a non-user the first e-mail will have a link that allows the non-user to put the e-mail on a hashed "block" list - When the non-user does not click the link, FB generates an array that lists all other users that have imported the same non-user ("shadow profile" of the user for "people you may know")

	- We do <u>not</u> believe that it can be seen as an "unambiguous consent" of a non-user to create a "shadow profile", if he does not click on the "unsubscribe" button in a small and gray text at the end of the e-mail. - We see the "array" that Facebook creates if a user does not click the "unsubscribe" button as the technical implementation of what we named a "shadow profile"	- Facebook interprets the fact that the non-user has <u>not</u> clicked on the "unsubscribe" link as an implied consent that allows FB to process the non-user's data for generating "friend suggestions" - The Hamburg DPC investigated this issue of contact importing and this process was decided in an agreement with them - It is up to the user to ensure that it is allowed to use this function within their jurisdiction (e.g. §45 Austria DPA) - Google, LinkedIn, Gmail do similar things!
03 Tags	**europe-v-facebook.org"** **-** Tags are "personal data" and allow finding and processing pictures or other content much easier for everyone. Therefore they cannot be seen as a solely "privacy friendly" technology. - There has to be a "specific consent" by the tagged data subject, this can only be obtained as soon as the data subject knows the specific picture he is tagged in. - "Freedom of expression" is not a superior right (like in the US) but has to be balanced with other fundamental rights (e.g. privacy) - Only controlling the "visibility" is not an option because there needs to be as much consent to "invisible" processing of data as is needed to visible processing of personal data. - Facebook has to implement a "tag request" system that allows the user to specifically consent to tags, or delete the tag request fully if they do not want to be linked to an object.	**Facebook** **-** Tags are good for the users' privacy because this allows them to find pictures of them on FB - The tagger is the controller of a tag - Tags are a form of "freedom of expression" just like when someone writes something about another person - The tagged person is able to control the visibility - By agreeing to the privacy policy the user consents to being tagged in any (future) picture on FB - This consent is "specific" enough no matter if the picture may be sensitive or unexpected - A user can control the visibility of any tag (hide it) - The fact that a user has removed a tag is stored to prevent retagging - There is currently no way of fully removing a tag - Users can also ask to have a picture taken down in certain cases <u>Follow up:</u> - FB is looking at whether to offer users the ability to remove the record of the removed tag; FB is unsure if this would be helpful given the possibility that a user might be re-tagged;

04 Synchronization *(see "02 Shadow Profiles")*	**-** Data that is not needed by Facebook should not be processed; "Processing" is defined as any action that is done with personal data (e.g. just uploading them to FB without storing it). - We are concerned about the access rights that FB's iPhone and Android apps have on users' cell phones (e.g. text messages, recent calls,…)	- There might have been more data transferred than only the name, e-mail and phone number, but it might have not been stored - Uncertain about phone applications abilities to access e.g. message information (see android market) <u>Follow up:</u> - Was there a change on the amount of information that is transferred from the iPhone-App to FB when syncing it? - Why do FB-Apps have rights to access e.g. text messages?
05 Deleted Posts	**europe-v-facebook.org** **-** There are still wall posst popping up on Mr. Schrems wall that were deleted and are <u>not</u> even in the data set. We are uncertain if posts are really deleted or just "hidden" from the user. **-** We believe that "wall" falls under the "first basket" and therefore the mere processor (FB) has to give options to the users to have reasonable/sensible control over the data (e.g. deleting options that allow to delete more than just individual objects).	**Facebook** - Deleted posts pop up because of a "bug" - Data resides in "hard to reach places" - FB intends to fully delete old posts - The deleted posts that were found in Mr. Schrems data set do not fall under the "90 days" exception for backups - FB thinks that users do not want "mass deletion" options (e.g. "delete all events / posts / … that are older than 2 months) <u>Follow up:</u> - Are old posts "deleted" or just "hidden"? - How does the deletion process exactly work?
06 Postings on other people's walls	**europe-v-facebook.org** **-** The data subject has to give an "informed consent" for every post since it is posted with a real name and therefore "personal data" - For giving such a consent, it is crucial to know if a post can be viewed by "friends" (e.g. 200 users), "friends of friends" (e.g. 40.000 users) or the worldwide "public" - If the user has consented to a post being only viewed by a limited number of people (e.g. "friends") the data controller is forbidden to chance the audience for the user - An information is not sufficient to replace the consent and will also result in a large number of notifications to users - We believe that the consent to "friends" or "friends of friends" is "specific" enough; There is no need to have an idea about the exact list of friends; This means that later chances to the friend list of the other user should be covered by the consent;	**Facebook** - The new „timeline" will soon have the proposed full information built in before a user posts on someone else's timeline **-** FB is still checking on the possibilities to implement the DPC's proposal for "information" when the audience gets changed and alternatives (e.g. not allowing users to choose a bigger audience once another user has commented on it)

07 Messages	**europe-v-facebook.org** **-** We do not believe that Facebook is on purpose gathering data in an excessive way, but we believe that the **outcome** of FB's message system is an excessive amount of personal data (given the purpose) - While normal IM services are **deleting** messages after a certain period FB is storing all chat messages on a central database - E-Mails and similar systems are usually stored in a **decentralized** way; This means that if a user is deleting the inbox and outbox it is practically impossible to assess the providers or users where the copy of an e-mail is still stored; - FB says it deletes a message only if all the users have actively deleted the message which in practice hardly ever happenes; The DPC was unable to assure that FB is actually doing so; - These facts combined make FB the only provider we know of that stores all communication in a long term centralized way; In addition, it is practically impossible for the individual user to fully delete personal messages; We think that **these facts combined** make this system a prime example of **excessive processing,** given the purpose (a chat); - Solutions would e.g. be a more decentralized system or a limited lifetime of chat messages	**Facebook** **-** FB does the same thing as any other e-mail / IM provider - FB does not use the content of messages for its own purposes - FB will improve the information on "deleted messages" and the analysis of messages - FB does not see the amount of centrally stored information that is still connected to a user after deletion by the user as "excessive" <u>Follow up:</u> - Is the traffic data used by FB? - If it is, for which purposes?

08 Consent and Privacy Policy	**europe-v-facebook.org** **-** We think that only actively ticking a check-box can be seen as an "unambiguous consent" when signing in to Facebook *(see D. Kelleher p. 210)* - Given the complexity of Facebook we doubt that there can be an "informed consent" to all functions when signing up the first time; Even long term users have a hard time to understand how many functions work; New users can hardly give a reasonable "informed consent" to all functions when logging onto Facebook the first time; - This means that there should be consent to all basic functions when signing up and additional consent (opt-in) when users choose to use further functions (e.g. applications, instant personalization, face recognition…) - There is more "specific" consent by the user every time they e.g. post something; - We do not think that simply changing the privacy policy in the background is sufficient to gain an "unambiguous and informed" consent to new regulations - Facebook's argument that there is enough information by the media is not sufficient to release FB from its obligation to get an unambiguous and informed consent by every data subject - The policies are so vague, lengthy and unclear that we doubt that a user has given an "informed, unambiguous and specific" consent when agreeing to it - Splitting the policy into different pages on FB is making it even harder to get a full overview of the policy; Full privacy policy is only available in English; - We think there has to be a clarification on who is the controller; This is the basis to e.g. decide who has to obtain consent by whom; - Given the "Lindqvist" case we doubt that FB is anything else than a host in most cases;	**Facebook** **-** Facebook have committed in the audit to improving the sign up process to make sure that users give an unambiguous consent to the privacy policy; - This might be done by having a "check box", but there are internal discussions with other "teams" within Facebook; - FB does not think that the European law requires the controller to generally implement an "opt-in" system - FB does not intend to change the current standard settings to less liberal settings - General consent is given by consenting to the privacy policy. More specific consent is given when using inline controls on the page - FB does not think it needs another explicit consent when changing the privacy policy - FB feels like users are aware of changes since they are broadly discussed in the media and published on its "site governance" page - FB believes that its process for notification and engagement of users in policy changes compare well with those used across the industry - A revised version of the worldwide privacy policy is expected by the end of Q1 2012 that will be clearer and more precise - FB plans to publish the privacy policy in a single document in all languages (currently this is only true for the English version) - FB does not want to clarify who is the controller in its policies; This has to be done on a case-by-case basis; - FB wants to be the "controller" of all function on facebook.com to be able to intervene whenever necessary (e.g. in cases of misuse)[1] [1] *Wording in FB's comment: "FB accepts that it will generally be regarded by data protection authorities as being the "controller" od data stored at facebook.com"*

09 Face Recognition	**europe-v-facebook.org** **-** We see the creation of biometrical face recognition data of potentially 800 million users as everything but an "incremental change" - FB did not ask the users for an "informed, specific and unambiguous" consent to activate the feature; - We think creating this highly sensitive data for its users is baring a tremendous risk to the users' privacy, given the limited purpose (a couple less clicks when tagging pictures) the data generated seems to be disproportionate to the purpose; We believe that this makes the feature a prime example of "excessive" processing; - The notice displayed in Jan 2012 was not equivalent to a consent; - The notice does not explain the process transparently; The process is not explained transparently, but is rather misrepresenting the facts; It is also not including the words "face recognition" or "biometrics";	**Facebook** - Consent given by agreeing to the privacy policy - Introducing the Face Recognition was an "incremental change" that did not make it necessary to have an explicit consent to the new policy - The tool is very well accepted; The number of people that opted-out of the face recognition is unknown; - When users choosing the "only me" option the biometric data of the user is fully deleted - FB does not use the biometric data for anything but suggesting tags to friends of the individual user - The feature is a massive help for tagging many pictures and therefore proportional to the personal data generated for it - There was a prominent notice in Jan 2012. The wording could have been more explicit, but FB sees it as sufficient to inform the users; It was only shown to users in the EEA since FB sees the information as an act of "best practice" and not as necessary by the law; Richard: "We tried to make it clear";

10 Access Requests	**europe-v-facebook.org** **-** Upon a request Facebook has to deliver a copy of all raw data that it holds of every user; We do not accept the currently discussed approach that will only deliver the "front end" data but not the background data (e.g. meta data of pictures); - The copy should be delivered in a tangible way (e.g. PDF /HTML file) that can be downloaded; We do not see the need for a CD; - The wording of the DPA and the Directive indicates that the data sets have to be "supplied" with the data; The currently discussed approach in the DPC's report means that the user has to go on a hunt for personal data all over the platform, this seems to be unacceptable; - We know that there is much more data than the 19 categories we named in our complaint; These 19 categories were just examples but not a final list of data; - The law does not provide for "trade secret" exemptions for the raw data; We do not accept a limited access to personal data; - Mr. Schrems would sign a NDA to enable FB to present evidence that certain data is not "personal data" without worrying for TS - Data generated by the "social plugins" are personal data and have to be included in the response to all access requests - If FB feels overwhelmed by the number of access requests they could have asked for the €6,35 fee it is entitled to by the Irish DPA - We do not believe that FB was unable to deliver the information within a reasonable time; The data Mr. Schrems got could have been automatically retrieved rather easily; - Simply ignoring the right to access is unacceptable	**Facebook** - "Most" data will be available on facebook.com - The implementation will take until the end of Q2 2012 - Information gathered via "Social Plugins" will be included - FB does not want to ask for the "access fee" as it would be possible under the Irish law - The 19 categories listed in the complaint are exactly the only 19 categories of personal data FB has no disclosed so far - Richard: "There are categories of personal data we have to disclose and there are categories of personal data we don't have to disclose"[1] - There were 4-5 requests a week before the campaign, but it is unclear if anyone ever got the whole data set before - The 40 day deadline in the Irish law was factually impossible to meet given the amount of access requests - It is unclear how long it took the employee to generate the PDF for Mr. Schrems <u>Follow up:</u> - We will receive a table of all categories of personal data that FB holds on its users, including a list of the contained data fields (covered by the right to access) - In cases where the right to access may be disputed we are willing to sign an NDA in order to be able to clarify the right to access - FB will not disclose any data categories that do not hold personal data [1] *additional comment:* *"…and the Irish DPC decides what data is in which category."*
11 Removal of Tags *(see "03 Tagging")*		

12 Data Security	**europe-v-facebook.org** **-** Our complaint is mainly based on the terms used by FB that indicate no responsibility for data security; We believe that these terms are generally not enforceable in many EU member states; -There is no other evidence that would indicate that FB is not living up to its obligations other than numerous media reports about breaches; - We were able to scrap information of about 200+ users for a project by the German TAZ newspaper;	**Facebook** - FB will assess the limitations on liability in its terms in response to europe-v-facebook.org's claim that they seem unenforceable within many member stated of the EU - FB will check on the possibilities of "scraping" (200+ profiles scrapped by the German "TAZ" to generate visuals)
13 Applications	**europe-v-facebook.org** - Applications can have numerous purposes and ways of functioning that determine the controller / processor role; - If a user exports his personal data he does not fall under the DPA; If the user exports third party data he is the controller; - There is no way that a third party data subject can give a "specific" and "informed" consent to the use <u>any</u> of his personal data by <u>any</u> friend, with <u>any</u> application, for <u>any</u> purpose under <u>any</u> privacy policy of <u>any</u> provider of applications on FB - There seems to be no way of enforcing the numerous contractual responsibilities of app providers, since FB is not even able to ensure on the most basic obligations (e.g. having a privacy policy) - The user is currently unable to ensure that an app provider sticks to the obligations it has as an processor / controller - This means that using most apps is illegal for European users	**Facebook** - FB sees the user as the "controller" for all actions that forward personal data from FB to the provider of the application - Consent is given by agreeing to the policy; It is further specified by the privacy settings of the user (opt-out); - FB explained the different forms of controls for users - This general consent is seen as "specific" enough by FB, even though this means any friend can forward <u>any</u> information to <u>any</u> controller of <u>any</u> application on FB - FB will ensure that all applications link to a privacy policy - FB does not keep a protocol of the data that is transferred between FB and an external application - App developers are regulated by privacy laws and the contract with FB as well - The user has to ensure that he is allowed to use such services under the European law (consent, Safe Harbor…)
14 Removed Friends	**europe-v-facebook.org** - We favor a full deletion at the first click - If users want to "block" further friend requests they should be able to actively put users on a "block" list - Preventive blocking of every user seems to be unnecessary in most cases and therefore excessive - If FB finds compelling reasons to retain the data for a certain period there should be a deletion routine after a certain time	**Facebook** **-** FB will improve the information about "removed friends" data - There will be an option to fully delete friends[1] - Data is kept so that the user is not suggested again but not for other purposes - FB does not intend to delete "removed friends" after a certain period of time *[1] In the comment by FB they said that FB is "…looking at offering users the chance to delete removed friends, but has questions about how useful this would be…"*

15 Excessive Processing	**europe-v-facebook.org** - The current privacy policy is more or less saying that FB processes all data it gathers for different purposes - If FB does in reality not process all data for all purposes this should be reflected in the privacy policy - The current approach that e.g. allows to process all personal data (incl. personal messages, all posts, all relationships, all deleted data), e.g. for targeting advertisement, seems to be excessive - We miss options to limit the amount of data that is stored by Facebook; Right now there is a lot of "junk data" that is very hard to remove for the user; Data that is not necessary anymore has to be removed according to the law;	**Facebook** - FB does not believe that processing all personal data it receives through the platform for its own purposes is "excessive" - FB will be clearer which data is / is not processed in its new privacy policy (e.g. content of messages, address book) - FB does not intend to introduce options for "mass deletion" (e.g. all posts/events/messages older than X months) since FB believes this not wanted by its users; FB thinks users may accidently delete information and maybe want it back later;
16 Opt-Out (see "08 Consent and Privacy Policy")		
17 Like Button	**europe-v-facebook.org** - Given the purposes disclosed by Facebook we do not believe that there is a need to collect personal identifiable data via social plugins - If the data is "personal data", it has to be included in the answer to any access request - There is no "specific" consent by users since they have no idea if there is a social plugin before visiting a web page - Users might have very different feelings about FB tracking e.g. activity on a news website or a porn website; A specific consent to tracking of all these different activities seems to be impossible;	**Facebook** - Data from "social plugins" can be "personal data" - The data collected when a logged-in user loads the button is linked to the UserID - The generated data is used to find bugs, to check on the success of a "like button" and to generate statistics for the page owner - FB is not using performance information of third party web pages - FB make retained personal data from social plugins available to the users (right to access) - FB gets consent to this use through its privacy policy; FB thinks this general consent is "specific" enough for logging the visits of all pages no matter of which content they are; <u>Follow up:</u> - Are there any other purposes for the collected data? - Page views may be included in "impression logs"?
18 Obligations as Processor *(see 08 Consent and Privacy Policy)*	**europe-v-facebook.org**	**Facebook** - FB does not believe it is a "processor" since the user is not a "controller"; Therefore it has no obligations as a processor

19 Settings of Pictures	**europe-v-facebook.org** - We do not think that the current approach of just controlling the access to the link to a picture but not the data itself is enough - We suggested that when a user limits the visibility of a picture to a more limited audience there should be a new "random number" generated in the link, so that the former link is not valid anymore - We are wondering if sub-processing by Akamai is legal (Safe Harbor)	**Facebook** - FB will check if changing the random number of the link to the picture would be a good solution whenever the number of people that can access the picture is reduced by the user <u>Follow up:</u> - Akamai USA is not in the Safe Harbor. Does FB-I have a contract with an EU subsidiary of Akamai or Akamai-USA?
20 Deletion of Pictures	**europe-v-facebook.org** - Pictures have to be deleted instantly; The user has given the consent to publish a picture knowing it can be deleted any time; Non-deletion is also not "fair" (see DPA) - Akamai's CEO said in an interview that they will enable deletion within seconds; Facebook should make sure that this includes all pictures and other user content;	**Facebook** - Photos will be deleted in a guaranteed 45 days. - 90% of the pictures will be deleted in a couple of minutes - There is the possibility for immediate deletion; Right now this is only used by FB for cases like e.g. pornography - The old system, that does not allow deleting pictures, will be shut down and moved to a newer picture system
21 Groups	**europe-v-facebook.org** **-** There is no unambiguous, specific and informed consent through providing an "opt-out" option - We suggest that users can send an invitation; The user should have the options to either "join" or "delete" the invitation; Only if the user actively "blocks" the group this fact should be recorded;	**Facebook** **-** Consent not necessary, because users have the option to leave the group - Users will be listed as "invited" until they first visit the group - The fact that a user has left the group will be stored to prevent multiple invitations, there will be NO possibility to fully delete the fact that a user has been invited to the group
22 New Policy *(see „08 Consent and Privacy Policy")*		