

europe-v-facebook.org

INVOLUNTARY

“Request for a Formal Decision”

Vienna, August 28th 2013

I. Introduction

1. History of my Complaints

On behalf of “europe-v-facebook.org”, Mag. Maximilian Schrems has brought 22 complaints before the Irish Data Protection Commissioner (DPC) against “Facebook Ireland Ltd.” (FB-I). FB-I is the legal entity running the social networking platform “facebook.com” for all users outside of the US and Canada.

In addition to this “two party” complaints procedure, the Office of the Irish Data Protection Commissioner (ODPC) has started an additional “audit” procedure that lasted about one year and led to the publication of a “report” in December 2011 and a “review of the report” in September 2012. The outcome of these reports are non-binding “best practice” suggestions for FB-I.

During the time of this “audit” procedure the ODPC has denied me any form of participation, has rejected “requests for a formal decision” and has only sent me the two audits as they were published on the internet. I was treated no different than the general public. I was especially unable to see any evidence, arguments or files of the case which made it impossible to intervene and defend my position. This issue was first raised with the ODPC in January 2012.

Numerous interventions, requests and letters were effectively ignored and did not change the situation of being “locked out” from my own procedure. The ODPC was unable to outline the procedures and was changing procedural rules every other day and at its own liking. Instead of clarifying the procedural rules the ODPC has usually referred to unspecified “previous communication” or has replied by general verbiage that did not clarify the issues raised. Explicit questions were factually ignored.

I was not part of this public “audit” procedure and the ODPC has in the summer of 2012 taken the position that the “audit procedure” was totally independent from my “two-party complaints” procedure. In recent letters the ODPC has now again indicated – as originally – that the “audit” was part of my complaints procedure. However, the ODPC has failed to clearly state the relation of these two procedures and is flip-flopping on this matter.

Because the “audit” in fact overlaps with the substance of most of my complaints the ODPC has asked me on September 21st 2012, if the outcome of the “audit” solves any of my initial complaints. To answer this question I have put together a very detailed “review of the audit”, sent to the ODPC on December 4th 2012. The ODPC has – as it did with all previous submissions – ignored this “review”. In addition I have (again) raised the issue that I am unable to make a “request for a formal decision” without having access to the files, evidence and arguments before the DPC. The only response I got from the DPC was the following:

“We do not wish to offer any comment on the enclosure. If you wish this Office to progress your complaints, you need to indicate clearly if and when you wish us to proceed with our standard complaint procedure which has already been explained to you (draft decision giving FB-I response etc.) and, if so, on the basis of your original complaints or some fresh (or reformulated) complaints.”

Overall the ODPC has consistently ignored any submissions, requests or questions and has only referred to their “outlined procedures”. The ODPC has also not undertaken any effort for an “amicable resolution” between me and “Facebook Ireland Ltd”.

After previously saying that it is at my sole discretion when I make a “request for a formal decision” the ODPC has on August 8th 2013 suddenly given me a deadline until August 30th 2013 (15 working days) to make such a “request”. Otherwise the ODPC would go ahead with the decision process without any further consideration. Even in the weeks before this letter the ODPC has repeatedly said that I have to make a request if I am unhappy. The ODPC has argued this latest change in procedural rules with by alleging that I would use the unsolved situation to harm the reputation of the ODPC.

In addition the ODPC has repeatedly said that it sees “Facebook Ireland Ltd” as being in full compliance with the law and thinks that the “audit” procedure has taken care of all issues raise in my complains. By doing so the ODPC has effectively taken a legal position despite the fact that I never had any possibility to comment on the procedure and all submissions were rejected. Therefore the ODPC has clearly left the position of an independent tribunal and is massively breaking any rules against bias.

However I do not see any other way than following through with this procedure under these unacceptable conditions and – under explicit protest – make this involuntary request for a formal decision. Otherwise I might lose any further possibility to submit my position in this procedure as all previous submissions were turned down and the ODPC has explicitly said that there will be no further possibility to submit any points made. At the same time I do not accept the way the ODPC is operating.

Currently I understand from the overall exchange with the ODPC that it is taking the following positions:

- a) The ODPC is operating under what it called an “informal procedure” and has not considered that it is a “tribunal” that has to live up to the standards of a “fair procedure” (e.g. Art 6 ECHR)
- b) The “audits” were a part of the complaints procedure – but I was not included in the procedure
- c) There was and will be no “amicable resolution” phase in the procedure
- d) There will be no exchange of arguments, evidence or access to files of the case at any stage
- e) I have to make a “request for a formal decision” until August 30th 2013 or otherwise I will lose the right to make any points that were not included in the initial complaints from 2011
- f) The DPC will send me and “Facebook Ireland Ltd” a “draft decision” and I will get the necessary time to review this “draft decision” and comment on it
- g) The DPC might include reference to arguments, evidence and files he relied on when making this “draft decision” and other arguments, evidence and files will not be referred to
- h) I will not be served the comment by “Facebook Ireland Ltd”
- i) After the comment period “Facebook Ireland Ltd” and myself will receive a final decision which is then subject to an appeal only on points of law to the circuit court and subsequently the high court

➔ ***R1: I am therefore requesting – against my free will – a “formal decision” on all 22 complaints filed before the DPC. This request is subject to the details outlined in this document and the requests, submissions and positions made or taken therein. As I am not getting any evidence, arguments or files of the case this request is not necessarily my final position and subject to further amendments.***

2. Summary of this “Request for a formal decision”

I have dedicated extensive resources and time to analyze and evaluate the “audit” by the ODPC and the meaning for my complaints procedure. I hope this (involuntary) request for a formal decision will lead to a decision by the DPC that will be in line with EU law and a “fair procedure”, despite the fact that the ODPC has already said that it sees “Facebook Ireland Ltd” (FB-I) to be fully compliant even before it has considered any of my submissions in the past two years.

I am happy to see that the “audit” has generally supported the facts I have brought before the ODPC. I was especially happy to see that I have no reason to correct any of my initial findings. A majority of the counterarguments by FB-I’s that I was able to derive from the “audits” were already expected and were even dealt with in my initial complaints.

I am also happy to let you know that some complaints are partly solved through the actions FB-I has taken in the last year. Most notably FB-I has changed the sign-up process, implemented deletion periods for certain data, updated the privacy policy multiple times, given users access to more data than before, and has suspended the facial recognition tools in the EU/EEA. To me this also indicates that my initial complains were fully justified.

At the same time I had to find that many facts or claims submitted by FB-I turned out to be false or at least not credible. In many cases I had to find that FB-I did not follow the suggestions in the “audit” or has simply submitted false or misleading evidence. The ODPC has relied on these facts and claims when making its decision, I therefore hope that the facts I am submitting through this review will also lead to a reevaluation of the “audit” by the ODPC, despite the position the ODPC has taken so far. I therefore hoping for an objective and credible reassessment of the “audit” procedure in all points raised in this (involuntary) “request for a formal decision.

3. “Audit” as a Solution for my “Complaints”

When analyzing the “audit” procedure I have recognized many steps that lead in the right direction and I hereby want to thank the ODPC for its work to achieve these steps. I am aware of the limited resources of the ODPC and I am happy to see that the points of discussions could be massively narrowed, but I currently see none of my complaints to be fully resolved.

In most cases the “audit” has simply not covered major parts of my complaints. In many cases the “audit” only named one of the reasons why I believed that a certain action by FB-I is illegal, but did not elaborate about other arguments I submitted. This is acceptable given the different scope and purpose of the “audit” and specific complaints, but this also means that the “audit” cannot be an alternative to a formal decision on my complaints. I can therefore only see that the ODPC has dealt with certain points of my complaints during the past two years, but has in no way made a full assessment of all points raised before through my initial complaints.

In some cases FB-I has simply not implemented the non-binding suggestions expressed by the ODPC in the “report” and the “review of the report”. As an example this is especially obvious when looking at the section on “access requests”: In my research it turned out that FB-I’s tools to let users access certain information are simply not working.

In some instances the “audit” has massively departed from the common European understanding of the law. National laws have to be interpreted in line with EU Directives. The EU Data Protection Directive (Directive 95/46/EC) has installed the “Article 29 Working Party”, representing all European DPCs to form a common interpretation of the law.

Many of the “best practice” findings in the reports are obviously contrary to the common understanding expressed in the documents of this institution. While the opinions of the “Article 29 Working Party” are not legally binding, we cannot understand how the “audit” can describe practices by FB-I that are contrary to these opinions as legal, or even “best practice”. We would need further clarification on why the ODPC has departed from this common understanding to be able to get a clearer picture.

In some cases the “audit” reports seem to be based on predictions, unproven claims by FB-I or general assumptions that lack fact-based evidence supporting them. I recognize that a facultative non-binding “audit” procedure might not follow more stringent forms of proof, but I see this as necessary to decide on fundamental rights in a two-party complaints procedure. I have indicated whenever question the evidence or claims in the following document and usually ask the ODPC to disclose existing or have FB-I produce evidence that would support these claims. I am sure that by getting this additional information I will be in a position to solve these complaints.

In relation to all complaints the ODPC has still not given me access to any of the arguments submitted by FB-I. I was also not allowed to access files or evidence concerning my complaints. As repeatedly expressed previously, I am left with almost no information in my own procedure.

This makes it factually impossible to have a “fair trial” and have a productive and meaningful procedure. The ODPC is deciding about very crucial constitutional and fundamental rights. If an authority is deciding about such core values this calls for an especially firm, transparent and fair procedure. I have dedicated the entire second section of this involuntary “request for a formal” decision to the “procedural issues”.

I know that the current situation might be extraordinary for the ODPC and I am happy to resolve any misunderstanding in this relation. I very much hope that the section in this documents and the broad and overwhelming analysis of the situation will eliminate the deadlock that I currently face and lead the way to a legally durable solution.

➔ ***Therefore I have to inform the ODPC that, while most complaints were narrowed down to the core questions, I am unable to drop any of the 22 complaints.***

➔ ***I am also unable to make a fully informed request a formal decision at this stage, because I lack the arguments by the other party as well as the majority of all files and evidence in relation to my complaints.***

4. Status of Complaints

In order to allow for a better overview I have indicated a status for all complaints in this table. As said before I see all my complaints as justified. In every case it seems that I the DPC has to establish further facts in order to be able to make a final decision. I have also indicated where it is clear from the evidence that major material steps were already taken during the “audit”.

No	Issue	Status of Complaint	Result of “Audit” Procedure
01	“Pokes”	Complaint Justified	No Proper Investigation/Evaluation
02	“Shadow Profiles”	Complaint Justified	No Proper Investigation/Evaluation
03	“Tagging”	Complaint Justified	Some Improvements
04	“Synchronizing”	Complaint Justified	No Proper Investigation/Evaluation
05	“Deleted Postings”	Complaint Justified	No Proper Investigation/Evaluation
06	“Posting on other Users’ Page”	Complaint Justified	Mayor Improvements
07	“Messages”	Complaint Justified	No Proper Investigation/Evaluation
08	“Privacy Policy and Consent”	Complaint Justified	No Proper Investigation/Evaluation
09	“Face Recognition”	Complaint Justified	Mayor Improvements
10	“Access Requests”	Complaint Justified	No Proper Investigation/Evaluation
11	“Deleted Tags”	Complaint Justified	No Proper Investigation/Evaluation
12	“Data Security”	Complaint Justified	No Proper Investigation/Evaluation
13	“Applications”	Complaint Justified	Improvements & Mayor Backdrops
14	“Deleted Friends”	Complaint Justified	No Proper Investigation/Evaluation
15	“Excessive Processing of Data”	Complaint Justified	No Proper Investigation/Evaluation
16	“Opt-Out”	Complaint Justified	No Proper Investigation/Evaluation
17	“Like Button”	Complaint Justified	No Proper Investigation/Evaluation
18	“Obligations as a Processor”	Complaint Justified	No Proper Investigation/Evaluation
19	“Picture Privacy Settings”	Complaint Justified	No Proper Investigation/Evaluation
20	“Deleted Pictures”	Complaint Justified	No Proper Investigation/Evaluation
21	“Groups”	Complaint Justified	Mayor Improvements
22	“New Policy”	Complaint Justified	No Proper Investigation/Evaluation

II. Procedural Issues

Continuing from my previous communication I want to (again) comment on the very problematic situation I am facing with respect to the denial of access to files, evidence and arguments concerning the complaints proceeding against “Facebook Ireland Ltd” (FB-I). Because I lack essential information I am unable to claim my fundamental rights. It is particularly impossible to enforce my rights without getting all counterarguments, evidence and files in relation to my complaints. I have to emphasize once more that the suggested “draft decision” is in no way sufficiently providing for a transparent and fair trial.

In Austria we enjoy a constitutional right to data protection (see § 1 Datenschutzgesetz). The right to data protection is also a fundamental right within the European Union since the enactment of Article 8 of the Charta on Fundamental Rights of the European Union (CFR).

According to Article 3 of Directive 95/46/EC this constitutional and fundamental right to data protection in relation to FB-I has to be enforced in Ireland. This is only possible from a constitutional perspective, because the core idea of Directive 95/46/EC is that there are equal laws in all member states *and* a coherent level of enforcement in within the EU/EEA.

It is hard enough to claim rights in a foreign language and legal system, but the idea of equal levels of data protection is totally undermined if the competent authority in one member state is in fact not enforcing these rights, or makes it factually impossible for data subjects to effectively claim their rights. In a broader sense it is crucial for the functioning of the entire European Union that citizens enjoy equal possibilities to claim rights under EU directives and regulations across different member states. There might be fields of law that have a different tradition or importance from one member state to the other, but it is crucial for the system of the Union that EU laws are enforced equally in all member states. Otherwise we would jeopardize such rights, undermine national constitutions and the rule of law. This would be in violation of Article 4 (3) of the EU treaty.

The current procedural obstacles make it actually impossible to effectively enforce my fundamental rights in Ireland and are thus causing an additional violation of Article 13 ECHR (right to effective remedy) in conjunction with Article 8 ECHR (right to privacy).

I have to stress that the DPC is a public, judicial tribunal that takes legally binding decisions at the core of these constitutional and human rights (see e.g. Article 8 ECHR, Article 8 Charta of Fundamental Rights). The ODPC has previously reacted to criticism on the fairness of the procedure with e.g. a text message or a press statement saying that the ODPS is *“disappointed that [I am] unhappy with the level of service it has received”*. Such reactions may be appropriate if people complain about a cold coffee at Starbucks, but in respect to fundamental and constitutional rights this leaves me with the impression, that the ODPC does currently not see its crucial function regarding such rights.

Regarding my complaints against FB-I the DPC is the judicial tribunal which is deciding on the protection of my fundamental rights, but also effects millions of citizens in the EU and about 190 countries worldwide. This responsibility of the ODPC calls for a very firm and transparent decision making process.

I have taken substantial effort to research my rights under the three legal regimes that govern the ODPC. I am hoping that this will help to overcome this situation and I hope the ODPC will grant me a fair and balanced proceeding. I also hope this will enable me to go on with the proceeding in a way that is fully compliant with Irish and European principles for a fair procedure.

1. Right to access Files, Evidence and Arguments

As previously mentioned I am aware of the different legal system (common law and statutory law), costumes and culture in the Republic of Ireland compared to Austria.

Even though it is very hard for an average citizen of one member state to dive into the legal sphere of such tremendous difference, I have invested substantial time to intensively research the Irish administrative law. After additionally consulting Irish experts I came to the following conclusions:

Two (overlapping) Proceedings

My complaints are a two party procedure under section 10(1)(b)(i) DPA. After I filed my complaints the ODPC has decided to start an additional public investigation (“audit”), which is based on other provisions like e.g. section 10(1)(a) DPA and partly even based on agreements with FB-I.

Up to date I have never received a clear statement regarding the relation of these two proceedings. The ODPC has (very likely for efficiency reasons) decided to conduct both overlapping proceedings at the same time, but has failed to define which action is serving which procedure. I understand that most actions by the ODPC served both proceedings, while some only served one of the two proceedings. The following analysis is looking at evidence, files and arguments that were either produced in relation to my complaints only, or for the complaints and the audit (“dual purpose” documents).

A. Right to access Files, Evidence and Arguments under Irish Law

DPC is a “Tribunal”

The ODPC has so far not answered my questions aimed at understanding which exact type of a public authority the DPC is. In an e-mail from the July 6th the ODPC has let me know that it “*never had to consider whether [it is] a Tribunal*”. In further correspondence the ODPC has not reacted to this issue.

I have repeatedly expressed my view that the DPC is a “tribunal” (an administrative body that decides on civil disputes between individuals). I recently found that my view is also shared by Irish scholars [see e.g. Hogan/Morgan, 4th ed., 2012, page 156].

In addition I have found that under Irish law “*a tribunal is always subject to constitutional justice in its more stringent form*” [see Hogan/Morgan, 4th ed., 2012, page 180] and that “*it is an element of a tribunal that, irrespective of the subject matter it should observe a fairly formal procedure*” [see Hogan/Morgan, 4th ed., 2012, page 469].

Decision about Fundamental Rights

In addition to the fact that tribunals are (independently from the subject matter) subject to constitutional justice in the more stringent form, I want to point out that the DPC is deciding on fundamental rights that are at the core of Article 8 ECHR and Article 8 of the CFR. There is no doubt that cases concerning fundamental rights must be reached under a particularly stringent, transparent, fair and balanced procedure, compared to an average tribunal.

In addition the Irish law does not allow for an alternative way to enforce these rights other than through the DPC. While other member states know alternative law suits (e.g. through ordinary courts) the Irish law only allows for a complaint to the DPC. Following the lack of an alternative the DPC has the burden to facilitate data subjects with a procedure that is allowing for enforcement in line with all principles of constitutional/natural justice in the most stringent form.

No written Provisions

As outlined before the Irish Data Protection Act (DPA) does not provide for a consistent and clear procedure, but is merely naming certain cornerstones and rights. There is also no general law on administrative procedure in Ireland.

I have learned that in Ireland issues that are not covered by the statutory law must be “filled” by general principles or case law to ensure compliance with constitutional/natural justice. The same procedure was undertaken by the Supreme Court in *EMI Records (Ireland) Ltd & ors v Data Protection Commissioner*, when the court has assessed general principles to find in what detail reasons must be given. This is in contrast to claims by the ODPC that in such situations only the (little) statutory rights apply and the ODPC would be free to decide on its procedures in all other respects. In fact the Irish system requires public bodies to act beyond the statutes to be compliant with general common law principles.

See e.g.: “State (Irish Pharmaceutical Union) v Employment Appeals Tribunal”:

“... If the proceedings derive from statute, then, in the absence of any fixed procedures, the relevant authority must create and carry out the necessary procedures; if the set or fixed procedure is not comprehensive, the authority must supplement it in such fashion as to ensure compliance with constitutional justice ...” [taken from Coffey, 2nd Ed., 2010, page 85]

This means that nothing is keeping the ODPC from granting me full access to all files, evidence and arguments in relation to my complaints. To the contrary the ODPC is in fact obliged under Irish common law to supplement in the statute to ensure compliance with constitutional and natural justice.

The ODPC has previously claimed that Article 28 (7) of Directive 95/46/EC is not allowing such disclosure. I want to mention that according to my research this section is interpreted in the opposite way by other member states when it comes to “two party” proceedings between a data subject and a controller. After getting in contact with different DPCs all over the EU, I have not found a single member state that only offers a “two party” proceeding before the DPC, but does not allow such disclosure.

Constitutional Justice / Natural Justice

In respect to the right to access to files, evidence and arguments, the constitutional justice principle of “*audi alteram partem*” seems to be applicable in many different forms, of which I want to name three:

First, the principle includes the direct duty of the tribunal to disclose all relevant material:

“A person affected ... must be given details of any information or advice received by the public body or tribunal outside of the hearing” [Coffey, 2nd Ed., 2010, page 84] or *“All documents and other relevant material must have been disclosed to the applicant ...”* [Coffey, 2nd Ed., 2010, page 96] or *“all information relevant to the issue, including details of the case against and in favor of the person affected”* [Hogan/Morgan, 4th ed., 2012, page 420]. The current Irish discussion goes even further *“the entitlement*

[to see relevant information] *extends beyond the bare case against the applicant and embraces other relevant documents and contextual material*" [Hogan/Morgan, 4th ed., 2012, page 421].

Secondly, the principle says that an applicant must be facilitated to make the best possible case:

If I am not getting the relevant evidence, arguments and files, but only the once the ODPC sees as "relevant" I am deprived of using material that is not supporting Facebook's (or the ODPC's) position. A perfect example for this is that the first two "reports" contain numerous findings that are contrary to the evidence I have submitted. Currently I have no possibility to elaborate and question these findings of the ODPC, since the basis for such (unexpected) results is not disclosed. In different variations it is logically impossible to make the "best possible case", if documents are not disclosed.

In addition I want to mention that according to previous communication the ODPC has forwarded my complaints and the submitted evidence to FB-I. While I have made much of the complaints public on our web page, there were other parts that were not made public. To my understanding the ODPC has delivered the whole complaints to "Facebook Ireland Ltd", which would constitute a massive imbalance between the treatments of the two parties before this tribunal and shift the equality of arms and the preconditions to make the best possible case favoring FB-I.

Thirdly, the principle to get information obtained outside of a hearing:

The ODPC has told me repeatedly that FB-I's law firm ("Mason Hayes & Curran") has submitted very excessive and defensive material in relation to my complaints in the autumn of 2011. Such information, as well as e.g. information that was obtained during the (five) "on sight visits" constitutes information that was obtained outside of the hearing before the ODPC. Such information must be disclosed, no matter if beneficial or adversely affecting my position.

Appeals Process

During my visit to the ODPC on May 25th 2012 I was told by Gary Davis that all evidence, arguments and files would be presented to me when I appeal the decision by the DPC to the Circuit Court and that there would be full access to all relevant documents at this stage. This claim was later not repeated by other colleagues of the ODPC, which is why I assume that the ODPC has dropped this idea. In any case such an arrangement would not be in line with Irish law: *"...the applicant is entitled to constitutional justice at the initial stage..."* [Hogan/Morgan, 4th ed., 2012, p. 472].

In addition to this I had to learn, that the Irish courts have so far ruled, that the appeal against the DPC is only possible on "points of law" and only on "serious and significant error of law" (see Novak v. Data Protection Commissioner, unreported). I am uncertain that this very limited scope of an appeal is in line with Directive 95/46/EC and the DPA but for the matter of this document, I have to stress that if there is a limited appeal there is no use for documents at this stage. As I would be unable to raise any factual questions at this stage anymore.

If the DCP is not disclosing the relevant files, arguments and evidence this would lead to another massive breach of the *"audi alteram partem"* principles and the general principles of a fair trial: The DPC would

have all documents in an appeal proceeding and have full oversight, while I would only have a fraction of the necessary information. There would be a drastic imbalance in chances to appeal any decision. In fact it would be almost impossible to file a meaningful appeal without knowing what has actually happened in the proceeding before the DPC. I would also be unable to assess the chances of different legal moves.

- ➔ ***F1: In summary a “draft decision” where only hand-picked parts of evidence, arguments and files are referred to is clearly not compliant with the principles of Irish natural/constitutional justice in relation to quasi-judicial tribunals where fundamental rights are at stake.***
- ➔ ***F2: In addition the principles of a fair trial are massively breached during a possible appeals process against such a tribunal.***

B. Right to access Files, Evidence and Arguments under Article 6 ECHR

Application

As mentioned before, the ODCP has to respect the obligations of the European Convention on Human Rights (ECHR) since Ireland is a signatory state of the Convention. In previous communication the ODPC has expressed the view, that the ECHR is not “national law” and therefore “does not apply to it”. I have researched this issue and want to direct the ODPC’s view to the Irish “European Convention on Human Rights Act 2003” (ECHR-Act), which transfers the duties under the ECHR into domestic Irish law and applies to “*every organ of the state*” [see section 3 ECHR-Act]. The DPC is undoubtedly such an “organ” and is therefore bound by the ECHR. The Act is not only transferring the ECHR into Irish law, but also declares the opinions, declarations and judgments of the ECtHR as binding for any such organ. Therefore the DPC has to observe the rights under the ECHR and the case law by the ECtHR.

Civil Dispute

As the cornerstone of modern proceedings Article 6, paragraph 1 ECHR (“fair trial”) applies to all tribunals that decide in a civil matter. This covers all civil and administrative disputes based on national (or EU) law between two individuals. The wording of the ECHR is independent of the national understanding of e.g. “civil” or “administrative” matters and was interpreted convention-autonomously very broad, reaching into many fields that are traditionally understood to be “administrative” matters.

Besides traditional civil rights, like the “right to privacy” or different “personality rights” Article 6 ECHR embraces e.g. limitations in building codes in the interest of a neighbor [e.g. “Ziegler v. Switzerland”]. The application of Article 6 ECHR is also independent from the national enforcement system and covers “quasi-judicial tribunals” (like the DPC) as well as ordinary courts.

Regarding my proceedings before the DPC, laws which guarantee the right to data protection between individuals would be: Article 8 ECHR, Article 8 CFR, Directive 95/46/EC (which is explicitly applicable between individuals) and the Irish DPA (which is directly applicable between individuals).

With view to the case law of the ECtHR there is no doubt that my complaints proceeding is a “civil” dispute. The complaints proceeding before the DPC is the only national framework under which these

rights can be enforced, it is not an optional “Ombudsman” proceeding. This means that the proceeding has to be compliant with Article 6 ECHR. [See also e.g. Jacobs, White & Ovey, *The European Convention on Human Rights*, pages 247f]

Right to access files

There is longstanding, well developed and undisputed case law by the European Court on Human Rights (ECtHR) concerning the access to all files, evidence, arguments and other submissions to a tribunal. In the numerous cases concerning criminal, civil and administrative matters the ECtHR is repeating (often even in a copy/past manner) the same principles:

1. The “*right to adversarial proceedings means in principle the opportunity for the parties (...) to have knowledge of and comment on all evidence adduced or observations filed with a view to influence the court’s decision*” [see e.g. “*Niederöst-Huber v. Switzerland*” p. 24, “*K.S. v. Finland* p. 21” or “*K.P. v. Finland*”, p. 25 and many more...]
2. The right was found to be independent from the possible influence on the outcome of the proceeding. “*Whatever the actual effect which the various opinions may have had on the decision (...) in the final instance, it was for the applicant to assess whether they required his comments*”. [see e.g. “*K.S. v. Finland*”, p. 23 or “*Vanjak v. Croatia*”, p. 56 and others...]
3. The right extends to all documents and evidence “*with a view to influencing the (...) decisions*” independent on the actual influence or the aim of the document [see e.g. “*H.A.L. v. Finland*”, p. 44, “*K.S. v. Finland*”, p. 23 or with other words “*Ziegler v. Switzerland*”, p. 38 among many more...]
4. The right does not only cover documents and evidence submitted by the parties but extends to documents and evidence that was “*obtained ex officio*” [see e.g. *K.S. v. Finland*, p. 19].
5. The right to access files, evidence and arguments is always based on Article 6 paragraph 1 (not paragraph 2 or 3). This means that it applies to all cases under Article 6, not only to criminal cases.
6. There may be limitations to the right to access based on legitimate interests of third parties.

In support of these principles see (among many others): “*K.P. v. Finland*”, “*Niederöst-Huber v. Switzerland*”, “*Kugler v. Austria*”, “*Ziegler v. Switzerland*”, “*H.A.L. v. Finland*”, “*K.S. v. Finland*”, “*Hrdalo v. Croatia*”, “*Atlan v. The United Kingdom*”, “*Ruiz-Mateos v. Spain*”, “*Lobo Machado v. Portugal*”, “*Vermeulen v. Belgium*”, “*Walston (No. 1) v. Norway*”, “*Rowe and Davis v. The United Kingdom*” or “*Dombo Beheer B.V. v. The Netherlands*”. [See also e.g. Jacobs, White & Ovey, *The European Convention on Human Rights*, pages 261f]

- ➔ **F3: In summary a “draft decision”, where only hand-picked or only “relevant” (according to ODPC) parts of evidence, arguments and files are referred to, is clearly not compliant with Article 6 ECHR.**
- ➔ **F4: The ECtHR is especially emphasizing that it is upon the parties to decide which documents are “relevant” and that a selection by the tribunal is in breach of Article 6 ECHR.**
- ➔ **F5: The “draft decision” approach is therefore also not complaint with the ODPC’s obligations under the Irish “European Convention on Human Rights Act 2003”.**

C. Duty to Provide for an effective Procedure under Article 8 ECHR

The European Court on Human Rights (ECtHR) has thus developed comprehensive case law (starting with ECtHR 8.7.1987, W. vs. UK; ECtHR 8.7.1987, O. vs. UK, ECtHR 8.7.1987, R. vs. UK) considering that every substantial guarantee of the ECHR contains inherently a minimum of procedural safeguards in order to serve an effective protection of human rights, such as to have legal standing or to receive substantial information regarding the alleged violation of those rights (see e.g. ECtHR 19.2.1998, Guerra and Others vs. Italy No 116/1996/735/932). Such inherent procedural safeguards have to be respected and provided independently of the applicability of Article 6 ECHR by applying Article 8 and Article 13 ECHR.

➔ **F6: The right to procedural safeguards, such as having a legal standing or receiving substantial information can also be derived from the ECHR, independently from the application of Article 6.**

D. Duty to Provide for an effective Procedure under EU Law

It is long standing case law and enshrined in Article 4 (3) of the Treaty on the European Union that member states (including all government bodies) have to ensure that EU legislation is carried out effectively:

“Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.

The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.

The Member States shall facilitate the achievement of the Union’s tasks and refrain from any measure which could jeopardise the attainment of the Union’s objectives” (Article 4(3) of the Treaty on the EU)

This does not only mean e.g. the transformation of directives into national law, but also includes effective enforcement of these laws by administrative and judicial bodies. Starting with the “Rewe” case (C- European Court of Justice (ECJ) has found member states to violate the treaties if the national implementation is not guaranteeing effective enforcement. This does not only cover the material law, but also the procedural law that is deployed by the member state. In countless decision the ECJ has repeated – word by word - the following standard test:

“54. However, the detailed national procedural rules governing actions for safeguarding rights which individuals derive from the direct effect of Community law must not be less favorable than those governing similar domestic actions (principle of equivalence) or render virtually impossible or excessively difficult the exercise of the rights conferred by Community law (principle of effectiveness)”
(taken ECJ e.g. from C-426/05)

In the words of the Advocate General:

“45. It must be emphasised, however, as the Court has held in the related context of the detailed procedural rules governing actions for safeguarding rights which individuals derive from the direct effect of Community law, that, although it is for national law to regulate this matter, that national law must comply with the requirements of the general principles of Community law.

In particular, the detailed procedural rules may not be less favourable than those governing similar domestic situations (principle of equivalence) and they may not render virtually impossible or excessively difficult the exercise of rights conferred by the Community legal order (principle of effectiveness).”

(Option of the Advocate General in C-426/05)

If the ODPC is now depriving me of any access to evidence, arguments and files concerning my 22 complaints, I am in a situation where an effective enforcement of my rights under EU law (Directive 95/46/EC and Article 8 CFR) is factually impossible or at least massively hindered. Under the Irish legal framework it is (in absence of a statutory provision) upon the ODPC to deploy procedures that do not deprive citizens of other member states from the possibility to make their case.

Especially in the field of Data Protection it is almost impossible to fully understand the functioning of a system without getting the necessary documents by the provider of such services. I cannot in any legal way access the systems of FB-I to provide evidence. In many cases on antitrust law the ECJ has taken this in account when determining that it was “virtually impossible” or “excessively difficult” to provide necessary evidence (see e.g. C-526/04 or C-535/11).

➔ ***F7: There is an obligation of the member states (and its public bodies) to implement procedural rules in a way that allows citizens of other member states to effectively claim their rights.***

➔ ***F8: A denial of access to file, evidence and arguments by the DPC is clearly violating this duty of the Republic of Ireland under EU law.***

E. Section 10(1), Second Schedule, DPA and Art. 28(7) of the Directive

The only material argument I have so far received from the ODCP on this matter was contained in a letter from January 4th 2012 in which Billy Hawkes explained the following:

"The Data Protection Acts (Second Schedule, paragraph 10) provides that: "... the Commissioner shall not disclose ... any intonation .. that could reasonably be regarded as confidential without the consent of the person to whom it relates".

This provision impose a duty of confidentiality on the Commissioner and his staff and transposes Article 28(7) of Directive 95/46/EC ("Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.").

For this reason, reports of audits carried out by the Office (around 30 each year) are not published unless the organization conceded agrees (Most organizations we audit do not agree to publication; FB-I, exceptionally, did)."

However I had to find that no other DPC in Europe that offers a two-party procedure is in any way interpreting this section of the law to be a total ban on any form of disclosure of arguments, evidence or files of a case. In Austria the DPC is e.g. government by the "Allgemeines Verwaltungsverfahrensgesetz" (AVG) that rules in § 17 that parties of a procedure have full access to all files, evidence and most certainly the arguments of the other party. As always this is only limited if "legitimate interests" of another party are jeopardized (such as e.g. trade secrets).

If the Article 28(7) of Directive 95/46/EC would generally prohibit any form of access to files, evidence and arguments then all other member states legislation and all other DPCs in the EU would permanently break the law. I have to wonder why no one would have brought this matter up over the past 18 years where this Directive is in force.

The truth of the matter lies in the words "*could reasonable be regarded as confidential*" (DPA) and "*confidential information*" (Directive 95/46/EC). No reasonable person would understand that arguments and evidence that was submitted in a two-party procedure would ever be "confidential". There is no confidentially whatsoever in the legal argument made by another party. The only thing that could be "reasonably regarded as confidential" would be any form of "trade secrets" or maybe "security codes" and equally confidential information.

- ➔ ***F9: Neither the DPA not Directive 95/46/EC are in any way prohibiting to exchange all non-confidential information. Legal standpoints can in no way be seen as "confidential". Other files and evidence are also not confidential as a general rule, unless there are "trade secrets" or other legally recognized rights of confidentially involved.***
- ➔ ***R3: I hereby ask the DPC to explain if it has any reasons to think that all documents, submissions, arguments, evidence and files regarding my complaints are "confidential".***

F. Summary “Right to access Files, Evidence and Arguments”

From different remarks in public documents (e.g. the cover of FB-I’s section in the review) and the general importance of trade secrets in the common law sphere I assume that Facebook Ireland has influenced the ODPC concerning the disclosure of documents. If the ODPC has possibly pledged to FB-I not to disclose information I want to stress that it cannot be bound by a pledge that deprives another party of constitutional and fundamental rights und Irish and EU law as well as the ECHR.

→ ***R4: I hereby ask the ODPC to inform me about possible “deals” with FB-I concerning evidence, arguments and files in relation to my 22 complaints.***

Given the clear law in all three legal spheres that can be deployed in this case, I am asking the ODPC again to make clear which evidence, arguments and files were produced in relation to my complaints. From this on I might be able to distinguish between three types of arguments, files and evidence that are before the ODPC:

1. Most of the documents will be in relation to the overlapping issues of the audit and the complaints.
2. There might be some material that is outside of the scope of the audit, but within my complaints.
3. There might be some documents that only relate to the public investigation.

I accept that documents that only relate to the pubic investigation will not be disclosed and fall under Article 28 (7) of Directive 95/46/EC and the DPA (e.g. documents in relation to the “real name” policy of Facebook Ireland Ltd, which was not part of my complaints, but part of the “audit”).

I would also accept limitations to disclosure when fundamental interests of other parties are at stake (e.g. trade secrets). It is common practice to blacken sections or words of the relevant files and I am accepting such limitations if necessary to protect legitimate interests. However, I would not accept general non-disclosure of files because of legitimate interests of others. Moreover, I expect clear and transparent communication about such limitations.

→ ***R5: Therefore I hereby (one more time) request copies and disclosure of all evidence, arguments, files and submissions that were produced for (1) the audit and my complaints (“dual purpose”) or (2) in relation to my complaints only.***

→ ***R6: If the necessary documents are so far not produced I hereby ask the DPC to produce the necessary evidence and files or request from FB-I their arguments.***

As a final remark I also want to stress that it must be in the core interest of the ODPC to have a productive and meaningful complaints proceeding. Such a proceeding is (independently from the law) actually impossible without the possibility for both parties to exchange on documents and arguments.

<p>I want to inform the DPC hereby that I will file a JR with the High Court concerning this matter. You may avoid this by disclosing the necessary documents before October 1st 2013.</p>
--

2. First Hand Evidence (via Swedish Data Center)

In the “audit” procedure I had to note that the DPC is mainly relying on pure claims by FB-I. In some events the DPC has looked at the terminals at the Dublin office of FB-I, but in no event the DPC has looked at the actual servers and systems of FB-I or any processor operating on behalf of FB-I.

This has led to many cases where the DPC has relied on “facts” that have no other source of credibility than FB-I’s Irish law firm or employees of FB-I that have no means of accessing servers operated by “Facebook Inc” in the USA. It is very likely that no one in headquarter of FB-I in Dublin has a solid knowledge of the functioning of “facebook.com”. In effect the DPC has so far relied mainly on hearsay.

Consequently I was able to show that FB-I has made claims that are clearly false as the “material law” section of this document is clearly outlining. Cross-checks are clearly showing that the claims by FB-I are in no way credible. This also means that there is a high likeliness that in cases that are harder to cross-check FB-I has equally submitted wrong claims and evidence.

Data Protection law is usually suffering from the lack of evidence, since it is usually impossible to “look inside” of software or servers that are not within the jurisdiction. However on June 12th 2013 “Facebook” has opened a data center in Luleå, Sweden – so within the jurisdiction of the EU (<https://www.facebook.com/notes/lule%C3%A5-data-center/lule%C3%A5-goes-live/474321655969861>). This means that the DPC is able to get fist hand evidence on the matters that were so far only relied on “claims” by FB-I that did not go beyond mere arguments. It is unclear to me if the installation in Luleå is operated directly by FB-I or by “Facebook Inc”, as a processor for FB-I. However the DPC has the power to gather first hand evidence from these installations.

According to Article 28(6) of Directive 95/46/EC the DPC can request the Swedish data protection authority to exercise their powers to investigate the Luleå installation:

“6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.”

The Swedish data protection authority has the power to access the installation, the servers and gather all necessary evidence for the complaints procedure before the DPC. The Swedish data protection law expressly empowers the Swedish data protection authority to conduct such investigations:

*“The powers of the supervisory authority
Section 43*

The supervisory authority is entitled for its supervision to obtain on request

- a) access to the personal data that is processed,*
- b) information about and documentation of the processing of personal data and security of this processing, and*
- c) access to those premises linked to the processing of personal data.”*

As outlined before the DPC has a duty under EU law to provide an effective procedure. Given the nature of data protection law this can only be accomplished through first hand evidence.

→ R7: I hereby ask the DPC to produce first hand evidence via the Swedish authorities whenever it has so far only relied on hearsay or pure claims by FB-I as this is the basis for an effective procedure.

3. Effective, Proportionate and Dissuasive Consequences

In recent letters and a number of media reports the DPC has taken the view that it follows some kind of “light touch” enforcement, which is in effect only seeing an “enforcement notice” as the worst thing that could happen to a company if it was not responding to different efforts of persuasion by the DPC. However before this is happening, a company gets lengthy “assistance” to comply with the law. The ODPC has summarized the situation in a recent letter by the following statement:

“You will also be aware that the ethos of Irish Data Protection legislation is to bring organisations into compliance where/if required, using a combination of persuasion and formal enforcement mechanisms (including the power of compulsory audit and the power to order compliance under pain of criminal sanction).”

As far as I could see there are however no publicly reported cases in which the DPC has ordered a company to pay a fine or even managed to have criminal sanctions imposed based on the DPA and Directive 95/46/EC. There were only a small fraction of cases where tiny fines were imposed because of unsolicited calls, emails or text messages. In fact the DPC is not even able to fine a breach of the law, but only a breach of “enforcement notices”. This means the DPC has to first make the law “punishable” through an “enforcement notice” aimed at a specific controller.

There is no objective reason to comply with the law at first hand, if there are no direct consequences when a company is “caught” breaking the law. It is even more convenient and much cheaper for a company to have the DPC “explain” how to comply with the law than complying in the first place and have ensure compliance at its own expenses.

This is however not in compliance with EU law. The ECJ has held in endless case law that it is up to the member states (and their authorities) to implement “effective, proportionate and dissuasive” penalties if EU law is not further specifying penalties:

“65. According to that case-law, while the choice of penalties remains within their discretion, Member States must ensure in particular that infringements of Community law are penalised under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance and which, in any event, make the penalty effective, proportionate and dissuasive (see, inter alia, Commission v Greece, cited above, paragraphs 23 and 24; Case C-326/88 Hansen [1990] ECR I-2911, paragraph 17; Case C-167/01 Inspire Art [2003] ECR I-10155, paragraph 62; and Case C-230/01 Penycoed [2004] ECR I-0000, paragraph 36 and the case-law cited therein).”
(taken e.g. from ECJ in C-387/02)

→ **F10: Ireland has a duty to impose “effective, proportionate and dissuasive” penalties.**

→ **R8: I hereby ask the DPC to take into account EU law and ensure that the procedure against FB-I is not turned into a prime example that a breach of EU law is left without consequences.**

4. Principle against Bias / Decision on “complaints” during “audit”

A. DPC is Judge in its own Matter (Objective Bias)

The “audit” procedure was in fact mainly dealing with my complaints. In the first report from December 2011 the ODPC has even linked to the complaints on our webpage (europe-v-facebook.org). According to the section of the material observations of the ODPC only sections 3.14 to 3.17 are not at all related to my complaints, while sections 3.1 to 3.13 are related to my complains. This means that by the pages 80% of the chapters of the audit report are in some way dealing with my complaints.

Generally public bodies are rather reluctant to change positions, if this would mean that their previous decision was wrong. This is especially true if the very same servant has to overthrow its own decision in a proceeding that involves massive national and international prestige.

In my concrete case the same public body and very likely the very same civil servants that have already decided upon them in the “audit” proceeding, will take the final decision concerning my complaints. Despite my repeated efforts to contribute to the audit and my repeated requests to take part in the process I was not allowed to take part in any way, after filing my initial complaints. If I am bringing new facts, evidence and arguments into the decision process, this would also mean that the ODPC was not itself producing such documents, was maybe even overlooking things or not taking everything into account, given the fact that the ODPC has so far said that the audit goes beyond the initial complaints.

If the ODPC would follow my claims, it would have to overthrow its own conclusions in the audit report. This means the ODPC might have to find itself and its “audit report” to be wrong or incomplete when following my complaints. In summary the ODPC is, when deciding about my complaints not only deciding about a dispute between “Facebook Ireland Ltd” and me, but also deciding on its own reports, audit and conclusions. In substance the ODPC objectively becomes the judge in its very own matter.

To avoid such situations procedures are timed and designed in a way that the same cause is only decided once by the same body and after prior involvement of all parties. The ODPC has decided to conduct two separate procedures on the same material questions at the same time, without the involvement of one party, which has led to these problems.

We are thereby finding ourselves in a textbook example of a situation where the *principle against objective bias* under Article 6 ECHR and Irish natural/constitutional justice is violated. This does not mean that there must be a situation of *actual* bias, but this is irrelevant under the law. The current situation is falling under all types of *objective* bias that one can e.g. find in Hogan/Morgan, 4th ed., 2012, pages 386f. In essence the ODPC is risking that any decision may be found to be void by the courts.

- ➔ **F11: The DPC is becoming a judge in its own case when it has to decide about the results it has produced itself during the “audit” and is thereby violating the “rule against bias”.**
- ➔ **R9: I hereby ask the DPC to resolve this issue in a way that an independent unbiased person is taking the final decision on my complaints. I am objecting to a procedure in which the final decision will be taken by any person that was involved in the “audit procedure”.**

B. ODPC has explicitly taken a position before the finding (Factual Bias)

The ODPC has expressed legal opinions on all 22 complaints before I was involved in a legal proceeding in any way (other than submitting the initial complaints). In summary the ODPC has already decided on my complaints before I was even (at least remotely) able to make my case. The DPC has even publicly declared that to his understanding my complaints should be decided upon:

"We would hope that the problems reported in the review will in fact have dealt with them, because we took account of the substance of these complaints." (Billy Hawkes, press conference, Sept. 22nd 2012)

In a recent letter from August 8th 2013 the ODPC has made it clear that without any consideration of my submissions and without any participation in the procedure it has already reached the conclusion that FB-I is not only fully compliant with the Irish DPA and Directive 95/46/EC but is going even beyond compliance by implementing what the ODPC called "best practice":

"As you will be well aware, this Office following completion (and publication) of a detailed audit of Facebook-Ireland in 2011 and a follow-up audit during 2012 to ensure implementation of the "best practice" recommendations made during the initial audit, considers that Facebook-Ireland are fully compliant with Irish Data Protection Law. You will also be aware of our position that, through seeking a "best practice" approach, an outcome was achieved which resulted in Facebook-Ireland going beyond mere compliance on many issues. (...) In the case of Facebook Ireland we consider that full compliance has been achieved through implementation by the company of the "best practice" recommendations made through the formal audit process."

This makes it clear that the ODPC has taken a position during the "audit" process that it now applies to my "complaints" procedure, before there was any form of an adversarial hearing or exchange or arguments of the parties before it. The complaints procedure is turned into a total farce if the ODPC is explicitly taking the position of one party, before it has even engaged in an attempt to find an "amicable resolution" as the first step of the complaints procedure under the DPA. All further steps the ODPC is engaging after this *forced* "request for a formal decision" can only be viewed upon as a charade that has no other purpose than pretending to engage in a "fair procedure".

Through these actions the ODPC has (additionally to breaching the *principle against objective bias*) also shown that it is obviously factually biased. While the previous comments by Billy Hawkes could have been accepted in one or another way as a mistake in excitement of a press conference, the most recent letter from the ODPC makes it impossible for me to pretend that this procedure is still fair and unbiased. It seems the ODPC only wants to "tick off" the rest of the procedural steps to get the case off the table, but is not even trying to pretend that there is a "fair procedure" that would be upheld in courts.

→ ***F12: The DPC has already made clear and explicit statements about its legal view before considering my arguments and having any form of an adversarial hearing. The ODPC has therefore turned the rest of this procedure into a farce and shown obvious factual bias.***

→ ***R10: I hereby ask the DPC to resolve this issue in a way that an independent unbiased person is taking the final decision on my complaints. I am objecting to a procedure in which the final decision will be taken by any person that has already taken a clear position on this case.***

III. MATERIAL ISSUES

1. General Remark: Article 29 Working Party Opinions

As I repeatedly refer to the working papers (WP) of the “Article 29 Working Party” throughout this document, I want to submit the following general remarks regarding these documents:

First of all I want to stress the importance of a common understanding of the European law and an equal level of data protection and enforcement throughout the EU/EEA. Besides ensuring the right to data protection, the core idea of Directive 95/46/EC is a free flow of information and a fair competition, through equal levels of data protection in our common economic area.

As a form of ensuring a common understanding and application of the law, the “Article 29 Working Party” has the function to form common opinions on questions of general importance (see Article 30 of Directive 95/46/EC). While the published opinions of the Working Party are not legally binding, they must be seen as guide line by the member states, everything else would make this institution obsolete. In addition I also understand the opinions to be the common understanding within the EU of the meaning of Directive 95/46/EC. Since the national law has to be interpreted in line with EU directives, I generally assume that the published opinions are a strong indication for the national interpretation and should be followed by national authorities, when enforcing the national laws. This general thought does not mean that there cannot be individual circumstances that would make it possible or even necessary to depart from this common understanding (e.g. specific national provisions).

The DPC follows some sort of a “best practice” model in its reports, which it claimed to be more stringent than the letter of the law. Considering this I believe that FB-I should at least be compliant with the relevant working papers, since they represent the common understanding of a “minimal standard”. Anything else could hardly be “best practice” but would rather be just “some practice” that is incompliant with Directive 95/46/EC.

I have very much welcomed that the DPC has partly followed WP193 when dealing with the “facial recognition” tool by FB-I. At the same time I could only see very little reference to other working papers that seem relevant to my complaints. I have decided to bring these documents in, since they could possibly be helpful when solving different legal questions. I would be very happy if the DPC could explain why it is departing from this common understanding of the directive, whenever a decision or position does not seem to be in line with the relevant WP.

- ➔ ***F12: The published opinions of the Article 29 Working Party form a common understanding of the directive and national laws should be interpreted in line with them.***
- ➔ ***F13: A “best practice” solution cannot possibly be incompliant with the minimal level outlined in the relevant WP. Instead it should follow the suggestions in the most stringent form.***
- ➔ ***R11: I hereby ask the ODPC to outline when and why it departs from the common understanding of the Article 29 Working Party.***

2. General Remark: Controller

One of the most crucial bases for any legal analysis is to find the entity or person that is responsible for a particular action. There is no substantial part of the report dedicated to this principal question, despite the fact that this issue is highly disputed (see e.g. the opinion by some German DPCs or many papers by scholars). The report refers to WP163, but this working paper does not hold any blanket rules for any social network. Therefore a clear answer for facebook.com cannot be derived from it without further observations and interpretation. After working on these complaints for 2 years, I want to make a couple of remarks on this issue:

A. Relation “Facebook Inc. (USA)” / “Facebook Ireland Ltd.”

While my initial complaints were based on the understanding that “Facebook Ireland Ltd” (FB-I) is the controller of facebook.com for all users outside of the US and Canada, I have to mention that during the last 2 years there were certain doubts that rose. During our talks with FB-I and its representatives we repeatedly heard that certain things are not possible because the management of “Facebook Inc” (the US parent of FB-I) would never agree to them. In other cases I had to see that Facebook employees in Europe have not even a remote knowledge of the systems and software that are run by “Facebook Inc”. It seems that the European offices only need to know what is necessary for their function (e.g. selling advertisement, user support or avoiding taxes).

This is raising the question how freely FB-I is deciding about the operations of facebook.com for all users outside of the US and Canada and is therefore itself “controlling” the platform that is technically hosted in the US. If not only the technical systems, but also the factual knowledge and control over the operations is exercised by “Facebook Inc” then FB-I would not be the controller, but just some operation, which only exists on paper and is mainly used to benefit from Irish tax loopholes. In this case FB-I would hardly be any more than the Offices in Germany, France and in other countries as they too do not have any factual control over the systems, but are merely functioning as “sales” or “support” agents.

The controller is defined as the person that has factual control. This means that agreements and contracts can only be an indication, but do not itself constitute controllership. I have serious doubts that FB-I might in fact not be freely deciding about the operations of facebook.com, but given the limited information I am currently not claiming that FB-I is not the controller. At the same time I would very much hope that the DPC can deliver some fact based evidence to make sure I am running a procedure against the right entity.

➔ ***R12: I hereby ask the DPC to produce or deliver fact based evidence that ensures that FB-I is actually the factual controller of facebook.com outside of the US and Canada.***

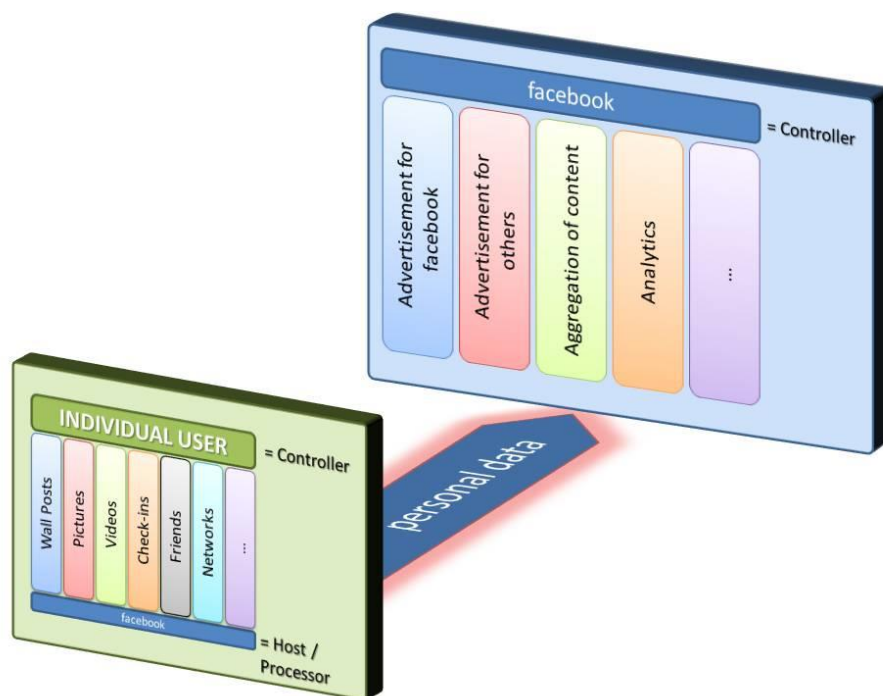
B. Relation Users / Facebook

Split Responsibilities and Powers

As I have outlined in my initial complaints, I have dealt with the question of the controller in detail and found a solution which I see as legally adequate and also produces reasonable results in relation to the duties of the users of facebook.com and FB-I. We need to get an understanding where the rights *and* responsibilities of the controllers are running parallel and reflect the factual reality. We also have to ensure that whoever is the controller must be able to adhere to the law.

As outlined previously, a Facebook page is in essence nothing other than a “blog” by a user that is hosted by FB-I. Equally like a “blog”, users can post pictures, videos and other people can comment to postings. This is nothing new compared to a usual relationship between a webhost and a user that runs a traditional homepage or “blog”. There is no doubt, that only the user controls the content of the page and that the host is e.g. not liable for illegal postings.

FB-I is not responsible for such activity, but might only need to take down data, just like any hosting provider of a usual web page. This understanding is commonly expressed when people refer to “my profile”, “my timeline”, “my messages” or “my data” when referring to their individual page or data on FB-I.



Left: User is controller of data, while Facebook is only Host; Right: Facebook is controller of further processing;

In addition to this first realm there is something “new” on facebook.com: FB-I, as the “host” of the first set of functions is also adding other functions that use the same data base, but cater towards other purposes than the users’ pages. FB-I is e.g. collecting users’ data to aggregate the “news feed” or uses the information to present personalized advertisements, to promote their service to non-users and many other such things. The user has no possibility to influence this second set of operations and can therefore

not be responsible for them. In fact the users are not even told what FB-I exactly does in relation to this second realm of operations.

If the Irish DPA and Directive 95/46/EC are applied to this form of a system, it is clear that we are looking at different “controllers” for different operations. The first realm of operations is done by the users and FB-I is merely hosting this information and providing the system. The users are therefore controllers and FB-I is the processor in relation to these operations (with “Facebook Inc” being the sub-processor). For the second set of operations are done and under the responsibility of FB-I. FB-I is therefore the only controller and “Facebook Inc” would be the processor, that runs the actual operations.

I also want to point to the wording of Section 1 DPA that defines the controller as *“a person who (...) controls the contents and use of personal data”* - it is undisputed that FB-I does not control the contents. This analysis is also in line with the wording of WP163 (page 5 and 6) that e.g. states that users are the controllers for pages and that they do not fall under the “household exemption” when a profile is shared with the general public (see the same reasoning in the ECJ’s *Lindqvist* case, C-101/01).

An equal understanding is shared by the Danish DPC, which claims that users of social networks are subject to Danish data protection law (<http://www.datatilsynet.dk/english/social-networks>). To my understanding this means that users are controllers or certain processing on Facebook.

Facebook’s Understanding

FB-I is generally opposing this system, at the same time FB-I was not able to suggest another approach that gives clear and reasonable results. In fact FB-I is flip-flopping when it comes to the responsibilities and rights towards the users’ pages. Whenever they want to have rights and power over the data they proclaim themselves to be the only responsible person, but as soon as there is a problem they suddenly shift all responsibility to the users. Here are some of the statements by FB-I during the past 2 years:

1. Meeting in Vienna

During our meeting with FB-I in Vienna, we have discussed this issue very broadly. After talking through this issue multiple times we asked Richard Allen, the representative of FB-I, who is the controller for data on facebook.com to their understanding. His final statement was:

“We are the controller for what we control... [and] ...the user has some responsibility too”

This statement is not only circular in nature, but is also reflecting FB-I’s reluctance to clarify the most crucial question of all, which is who has the final responsibility for what happens on the platform. In relation to the individual functions FB-I was not willing to give a statement on who they think the controller is. Only with some minor issues (e.g. when users import or export data via “apps”) FB-I was willing to take a position. Other than that FB-I was saying that the controller function has to be determined on a “case by case basis”, without doing so for the most functions in question.

2. New Policy and Public Statements

Following the interventions by the ODPC there was a major change of the privacy policy that FB-I is operating under. One of the changes was that FB-I is now claiming that it is the controller for all data.

"The website under www.facebook.com and the services on these pages are being offered to users outside of the U.S. and Canada by Facebook Ireland Ltd (...) Facebook Ireland Ltd. (...) is the data controller responsible for your personal information."

This triggered heavy criticism by our group, but also by other legal experts and other European DPCs. In essence this would mean that users are losing control over their data as soon as they post something on facebook.com. As FB-I had been claiming so far that *"all data belongs to the users"* this would be a dispossession of users. Different media has inquired about this claim, especially in Germany. As an example I want to cite the original statement from Robert Ardel, Speaker of FB-I in Germany in reaction to a question from the German TV show "Stern TV":

GERMAN Original:

Stern TV: Die Facebook-Kritiker "Europe vs Facebook" werfen Facebook vor, in den neuen Datenschutzrichtlinien der "Controller" aller Daten zu sein und damit den Nutzer zu enteignen. Was sagen Sie dazu?

Ardelt: Das ist ein Missverständnis. Wir nutzen das englische Wort „control“ um zu erklären, dass wir die Daten verwalten. In der englischen Fassung der Vorschläge heißt es dementsprechend, Facebook "is the data controller responsible for your personal information". Die Übersetzung "Dateninhaber" ist etwas unglücklich, "Datenverwalter" wäre treffender. Denn, um es ganz klar zu sagen: die Daten gehören selbstverständlich den Nutzern.

ENGLISH Translation:

Stern TV: The Facebook critiques „Europe vs Facebook“ are accusing Facebook to make themselves the „controller“ of all data in the new privacy policy and thereby disappropriating users. What do you say?

Ardelt: This is a misunderstanding. I am using the English term "control" to explain that I am holding the data. The English version of the proposal is therefore saying that Facebook "is the data controller responsible for your personal information". The translation "Dateninhaber" [German for "data keeper"] is a bit unfortunate "Datenverwalter" [German for "data administrator"] would be more accurate. Because to be very clear: all the data of course belongs to the users.

In a video chat that "Facebook Inc." published when the new policy was presented, Mrs. Erin Egan (the "Chief Privacy Officer-Policy" of Facebook Inc.) has made a statement that clearly stressed that only the user has the power over the individual page:

"Again: Another way we wanted to be really clear with users is.. Basically I control my space. So I control my timeline. I control the audience for things on my timeline... You control the audience for things on your timeline..." (Live stream at 11:30, See [Copy on YouTube](#))

This is also in line with the following section of the current privacy policy used by FB-I:

"While you are allowing us to use the information we receive about you, you always own all of your information."

Given these public statements (which are just some of hundreds) it is clear that FB-I has publicly and repeatedly stressed, that the users own, control and are responsible for their page.

Recently FB-I has repeated this claim in a posting (see left). FB-I clearly claims that

"...anyone who uses Facebook owns and controls the content and information they post, as stated in our terms. They control how that content and information is shared. This is our policy and it always has been."

In this statement FB-I says in no way that it has any rights to the data or is the sole controller in this statement.



3. Responsibilities for illegal Behavior

The power and control over a situation always go hand in hand with the responsibilities for any illegal activity or liability. It is an undisputed general principle that duties and rights are generally not to be separated. There is no reason why this should be any different in relation to social networks.

As a wonderful example I want to mention the case of a young Irish student, which has discovered that he had been wrongly identified as someone who had taken a taxi without paying. The CCTV video that was said to show him was spreading all over facebook.com and other internet services.

According to news reports FB-I has in essence claimed that it cannot be made responsible for whatever its users post on their pages, since they are unable to control and censor every posting. FB-I only acknowledged that it would take down illegal postings, which falls under its obligations as "host". In essence FB-I has exactly argued the same way as we did in the initial complaints and above.

Equally Richard Allen has argued in a "witness statement" before UK authorities that not FB-I but the users are responsible for what their users post and do on the platform. FB-I can only take down things and police certain things that were reported to it, or that triggered the systems. Here are some excerpts:

"Facebook operates both as a service that is delivered directly to users and as a platform on which others can build their own services. The service is made up of core site features and applications. Fundamental features to the experience on Facebook are a person's Home page and Timeline (formerly, Profile)"

"It is important to note that Facebook does not itself produce the content that is shared via its service."

"This is consistent with our view that people own the content they post on Facebook and have a responsibility for making judgments about how that content is shared on the service."

"Users of the platform have their own responsibility for the legality of anything they post."

(Original: levesoninquiry.org.uk/wp-content/uploads/2012/01/Witness-Statement-of-Richard-Allan.pdf)

Summary

In essence there is no doubt that not FB-I, but the users control the "first realm". For this "first realm" FB-I is only a host/processor. At the same time FB-I is the sole controller for everything that fits under the "second realm". The understanding of all further problems is based on this understanding.

- ➔ **F14: There is no evidence or statement by FB-I that would support the position in the "audit" that FB-I is the sole controller of the users' data.**
- ➔ **R13: I hereby ask the DPC to explain disclose and explain anything that would allow a different view, as this is a basis for any further assessment of the legal structure of "facebook.com".**

C. Household Exemption

I also want to mention that the “report” of the DPC has departed from WP163 when it comes to the rights and duties of the users. I miss a solid analysis and understanding of the users’ role. The “report” says that users are not controllers, but fall at the same time under the “household exemption”. This is not stringent, since only controllers can fall under the law and can subsequently claim a household exemption.

“Under Irish law where an individual uses Facebook for purely social and personal purposes to interact with friends etc. they are considered to be doing so in a private capacity with no consequent individual data controller responsibility. This so-called domestic exemption means for instance that there are no fair processing obligations ... for an individual user when posting information about other individuals...” (Frist Report, Page24)

I do not believe that a private user that posts personal data of other data subjects is exempt from the law unless it processing data in a small circle of only friends. A standard profile on facebook.com is “public” and therefore no different than a normal webpage. There is no reason why such a public profile should be treated any different than a normal webpage (see again the ECJ’s *Lindqvist ruling*, C-101/01). This is also in line with findings of the Danish DPC and the Article 29 Working party:

“When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected ‘friends’ data controller responsibilities come into force.” (WP163, Page 6)

➔ ***R14: I hereby ask the DPC to review this position and explain why the “Lindqvist” rationale would not apply to facebook.com, if third party data is shared with the general public.***

3. General Remark: Technical Report

Both reports are accompanied by technical sections. These reports are generally in line with my findings and seemed to have produced reasonable outcomes, which is why I see my claims generally supported by these reports. At the same time there are certain sections that seem to be only based on FB-I's claims or are impossible to verify independently. While I respect the confidentiality of certain trade secrets of FB-I or security relevant information, the DPC cannot base this proceeding on such findings.

➔ ***R15: I hereby ask the ODPC to disclose the evidence, arguments and files that the technical report is based on in so far as they relate to my initial complaints.***

In addition I want to mention that I was unable to find out more about the company doing the secondary analysis ("FTR Solutions"), other than the fact that Dave O'Reilly, who seems to be working for "FTR Solutions", has already conducted the analysis in the first "audit".

The webpage of "FTS Solutions" (www.ftrsolutions.com) does not have a legal notice. The URL is registered by "Domain Discreet Privacy Service" in Jacksonville, Florida, USA. Only a look at the Irish companies register returned an address of a residential house in Blessington, Ireland.

After additionally sending an email to "FTR Solutions" I only received the following response:

Thank you for your email. Concerning your questions, the status of FTR Solutions is a matter of public record and my personal LinkedIn profile is also in the public domain (<http://www.linkedin.com/pub/dave-o-reilly/6/322/b37>). For any issues relating to Facebook Ireland, I refer you to the Office of the Data Protection Commissioner.

Overall this amounts to little credibility of these findings as "FTR" seems to be a "one-man show" without any physical presence. In addition I am unable to talk to this "expert witness", I am unable to see the evidence this person has relied on and I am unable to verify his independence.

➔ ***R16: I hereby ask the DPC to give me a rough idea about the background of "FTR Solutions" and their status in the proceeding to verify the credibility and independence of this source.***

4. Complaint 01: “Pokes”

A. Facts described in the original Complaint:

The Facebook Platform gives every user the possibility to “poke” other users. This is in fact just a little message that is sent to the other user, who is then displayed the “poke”. The user may click a little “X” then the poke is not displayed anymore. The explanatory text to the little “X”-Button is “remove” (see screenshot in attachment 03).

The Oxford Dictionary defines “to delete” as “remove (data) from a computer's memory”, which clearly shows that by using “remove” the user expectation of “deleted” data is triggered. This is the same in many other languages the Facebook platform is available in. For example, the German version uses the word “entfernen” which is the name of the “delete”-key on any German keyboard. The user experience is that the “poke” is gone and not displayed in any way anymore.

Surprisingly Facebook send me a copy of all “pokes” I ever sent to others or received since I registered with them on June 8th 2008 (about 3 years ago). The oldest “poke” dates back to June 23rd 2009 (about 2 years ago). See the excerpt of my access request (attachment 04). Another user [...] who requested his personal data got about 58 pages of “pokes” dating between the 25th of January 2009 and the 7th of June 2011 (2½ years). All these pokes were already deleted but are still processed by Facebook Ireland (see attachment 05). In both sets of data it is easy to see that Facebook Ireland marks “removed” pokes only as “viewed”, but does not really “remove” these pokes.

Since any purpose of the “poke” for the user and all possibility to process the “poke”-data is gone at the time the user has clicked the “X”-button, any further processing of the “poke” is done by Facebook Ireland, which must be seen as the sole controller of all data in question.

Under the section of Facebook Ireland’s privacy policy (see attachment 06) which describes the use of data by Facebook Ireland (“5. How We Use Your Information”), the only information is that the data is used “to try to provide a safe, efficient, and customized experience.” This is only followed by some examples of this use, but by no explicit determination what is done with data like the “pokes” that Facebook Ireland collects.

B. Reaction by FB-I and the DPC:

The “audit” from December 2011 quotes the complaint and brings forward FB-I’s argument that the retention of more than two year old pokes is necessary to prevent “cyber bullying”.

It also says that “FB-I categorically denied that it engaged in any deception, although recognized that “remove” could have been interpreted by users to mean that the data was deleted” – a claim one could have interpreted as a tiny understatement by FB-I, given the clear meaning of the word.

In our meeting with FB-I in Vienna it was added that they have to be kept for *“all sorts of reasons”*, but FB-I was unable to tell us the exact purposes for which they are processed. In a follow-up letter by Richard Allen (FB-I) he also added that FB-I is using the deleted information *“for other purposes in connection with bringing the ... service to the users”*. The letter refers to the clause of FB-I’s policy that allows for any kind of processing:

“We use the information we receive about you in connection with the services and features we provide to you and other users, like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”

The DPC has asked FB-I to change its policy in the first “audit”: *“User’s should be provided with an ability to delete ... pokes, ... and be able to in so far as is reasonably possible delete on a per item basis.”* This meant to me that “pokes” are to be deleted instantly whenever a user “removes” them.

Unfortunately the second “audit” report does not elaborate about “pokes” but does only give some general wording about “retention”. Interestingly the second “report” says that the data had to be kept to protect users from *“re-poking”*. A function to protect against *“re-poking”* was never an option on facebook.com. Users were only able to “block” a person, but this does not lead to a need to keep old pokes. The DPC further only says in connection to all kinds of user data that *“Following extensive engagement, this Office and FB-I agreed that user control in this area could be extended so as to enable users to delete such items on a per-item basis”*.

However I was unable to see any difference if one deleted “pokes” from another user. I was unable to find any solid consequence as to how FB-I changed its system concerning old pokes in the September 2012 report. In our direct talks we were also not informed about how FB-I has changed or was intending to change the processing of “Pokes”.

This was also confirmed by the most recent tests we have conducted: After “removing” a poke, the information was still available in the “notifications” menu:



Screenshot from “facebook.com”

Because I am unable to see any arguments, comments, evidence or files concerning this matter, I have to assume that FB-I is still holding “pokes” after they have been deleted. The DPC has in no word said that it has confirmed that FB-I is deleting old “pokes”. I can therefore also not further elaborate if such a confirmation was done in a way that would give me proper confidence that FB-I’s way of processing “pokes” has changed in any way.

- ➔ ***F15: The only substantial counterclaim of FB-I why pokes are kept for an indefinite time (“poke harassment”) is surely creative, but legally absurd.***
- ➔ ***F16: I was not informed about any change in FB-I’s processing of “pokes”. From the experience on the web page it seems like “pokes” are still only “hidden” from users, but not deleted.***
- ➔ ***R17: I hereby ask the DPC to forward any additional information on this matter and inquire if FB-I is still keeping this information, how long it is kept. If the DPC is not further clarifying the facts, I assume that there are no other established facts than the once mentioned above.***

C. Legal Consequences described in the Original Complaint:

I do think this processing by Facebook Ireland is illegitimate under the Irish Data Protection Act and the Directive 95/46/EC for the following reasons:

- 1. There is no transparent notice that these bits of data are still held. In contrast to that, the user is told that the poke is “removed”, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
- 2. There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) DPA.*
- 3. There is no longer a legitimate purpose for holding on to these bits of data. There is no other purpose than the transfer of the information by these bits of data specified by Facebook Ireland. The data would have to be deleted according to section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
- 4. The further processing of this bits of data is no longer relevant for the purpose of the processing and seems to be also excessive, which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
- 5. The processing of the data seems to be longer than necessary to fulfill the purpose and therefore seems to be no longer necessary. This would constitute a breach of section 2(1)(c)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*
- 6. It seems that there has never been an informed consent by the user to the use of these bits of data since the user just agreed to the processing by having the option to “remove” this content later. If Facebook Ireland does not remove any of this content, the consent seems to be neither informed nor unambiguous and therefore void under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EC.*

D. Additional Statement concerning Legal Consequences:

Neither the DPA, nor Directive 95/46/EC allow mass storage of data without the consent of the data subject and for the mere possibility to prevent the rights of a user in a rather hypothetical situation (“cyber bullying via pokes”). While it is true that cyber bullying happens on facebook.com, like anywhere else on the internet, there are other solutions (e.g. by “blocking” the user) than keeping every little bit of information about every user. Otherwise most of the data protection legislation would be redundant, since all information could be possibly used for some hypothetical legal case.

In addition I want to mention, that the recipient (so the hypothetical victim of “poke bullying” situation) in this situation has deleted these pokes. If the victim e.g. wants to press charges because of “poke harassment” he/she can simply not delete the pokes.

The fact that FB-I has stored information, without a legitimate purpose and without a justification, without proper information and for an indefinite time constitutes a clear breach of the provisions of the Irish DPA and the Directive 95/46/EC as described in my Complaint 01 from August 18th 2011.

E. Summary:

I see my initial complaint to be fully justified. I was not supplied with any facts, arguments or evidence that would indicate otherwise. There is no reason to believe that FB-I has in any way stopped or changed what is clearly a violation of the DPA and Directive 95/46/EC.

- ➔ ***R18: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed in my initial complaint.***
- ➔ ***R19: I hereby – involuntarily – ask the DP to find that FB-I is continuing to violate the sections of the law listed in my initial complaint.***
- ➔ ***R20: In order to comply with the duty of effective enforcement under EU law (see above Part II.3), I hereby ask the DPC to take every measure possible to impose a substantial, effective and dissuasive penalty or other form of consequence on FB-I.***

5. Complaint 02: “Shadow Profiles”

A. Facts described in the original Complaint:

Facebook Ireland uses many functions that are targeted at getting more information than the actual data subjects are sharing on the facebook platform. Therefore Facebook Ireland collects as much information of users and non-users as possible. Facebook Ireland is mainly collecting e-mail addresses but it also collects names, telephone numbers, addresses or work information about its users and non-users.

This is done by different functions that encourage users to hand personal data of other users and non-users to Facebook Ireland (e.g. “synchronizing” mobile phones, importing personal data from e-mail providers, importing personal information from instant messaging services, sending invitations to friends or saving search queries when users search for other people on facebook.com).

Even commercial users that have a “page” on facebook.com have the option to import their costumers’ e-mail-addresses to promote their page (see attachment 03).

By gathering all this information, Facebook Ireland is creating extensive profiles of non-users and it is also enriching existing user profiles (see attachment 04). This is done in the background without notice to the data subject (“shadow profiles”); the user or non-user is only experiencing some of the result of these shadow profiles: There are “friend” suggestions by Facebook Ireland based on the information or non-users get invitations showing many users that they actually know in real life.

This means that Facebook Ireland is gathering excessive amounts of information about data subjects without notice or consent by the data subject. In many cases these information might be embarrassing or intimidating for the data subject. This information might also constitute sensitive data such as political opinions, religious or philosophical beliefs, sexual orientation and so forth.

Even in the answer to my access request, there was no information that would disclose this information to me, such as which people uploaded my e-mail-address or disclosed my personal data when they “synced” their phone with facebook.com.

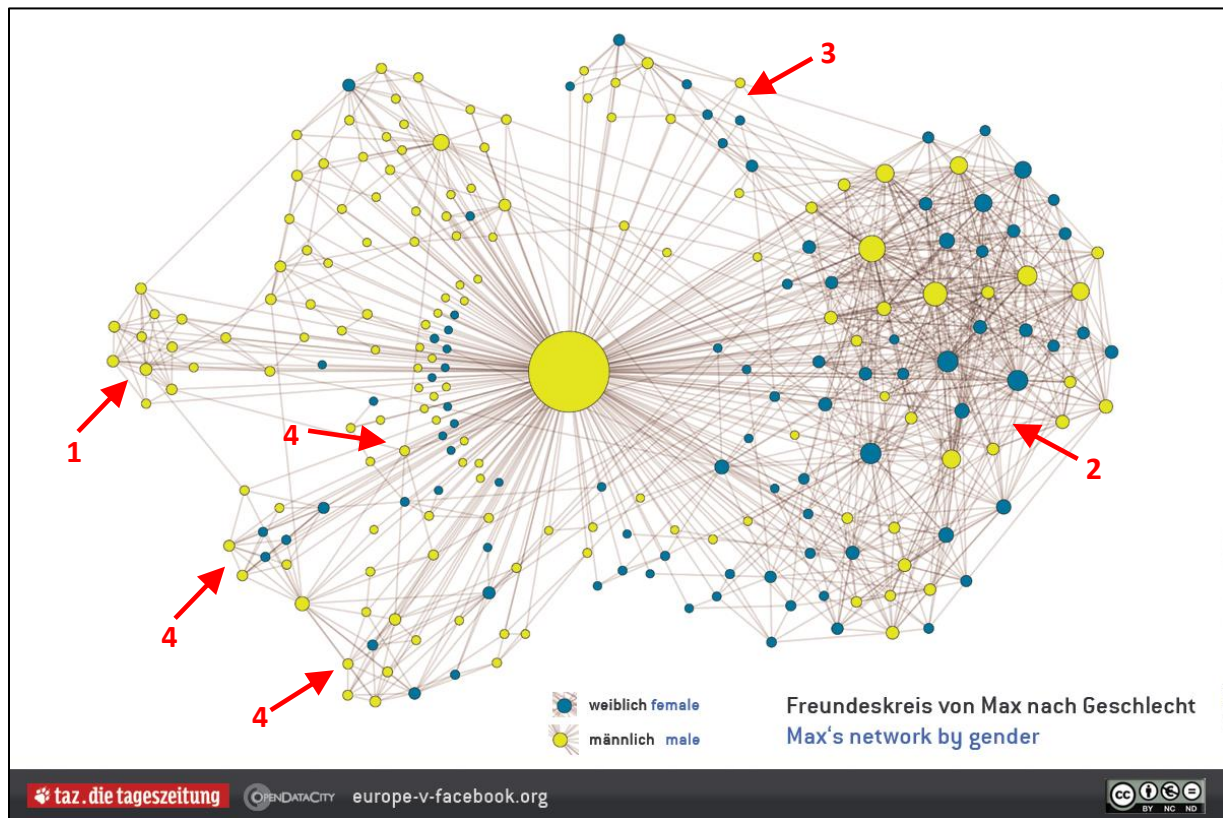
B. Additional Submission of Facts:

After conducting further research I came to the conclusion, that despite FB-I’s claim not to hold “shadow profiles”, there are far reaching data sets about users and non-users that are invisible to the data subject (which I have called “shadow profiles”). This can also be seen on a daily basis when invisible data is “surfacing” e.g. as “friend suggestions” or when things that are only related in the background are e.g. “grouped” on facebook.com. This “shadow data” enables FB-I to know much more about users than what they deliberately shared or exchanged via facebook.com.

When submitting the initial complaint I was unable to further specify the issue, but during the past year the phenomenon I have described previously became known as “**big data**”. After prices for processing and data storage dropped, companies have departed from a purpose based processing of data, but are instead deploying “web” systems that are able to connect seemingly unrelated data of millions of users with each other (“correlations”). I would therefor like to amend my complaint to expressly cover this issue, despite my understanding that already my initial complaint has described this phenomenon without using the word “big data”.

Network Analysis

As an example I want to submit the graphic below. It combines my friend list with the friend lists' of his friends. The result is a “web” that shows certain groups of friends. This (simple) graphic in connection with basic information about the friends allows e.g. to determine that he was serving his community service as an ET at the Red Cross instead of serving at the military (1), was a member of an NGO (2), stayed in a Muslim country for a longer time (3) or went to certain Universities and Schools (4). Other information (e.g. health, sexual orientation or political views) can be determined in the same way.



Relationship between different users, based only on 1 submitted and about 150 other 'scraped' friend lists.

This is a very basic graphic, only using friend lists, but it is already showing connections that a normal user cannot see, remove or amend when using facebook.com. In reality there are additional “hidden” connections to many more users (e.g. by searches, imports, address books, click data) that cannot be displayed in this graphic. Every dot is also not only a name, but again a whole Facebook profile. From this graphic one can e.g. see how FB-I can find out information about a user by analyzing what friends have shared or “friends of friends” have shared. In our tests it was easy to figure out the workplace, educational history or family members. But it was also possible to figure out sensitive data like political beliefs, sexual orientation or union memberships. All of this was never shared by a user. There is no form of informed or specific consent and no way to remove, amend or even just opt-out of such analysis.

In addition to such “big data” analysis, invisible data (click data, advertisement information, data from social plugins, protocols, IPs, friend finder data, administrative data, etc.) can be added to user. In addition general demographics can be added to the pool of information. In the background the “visible” data is connected with “invisible” data that might serve another purpose.

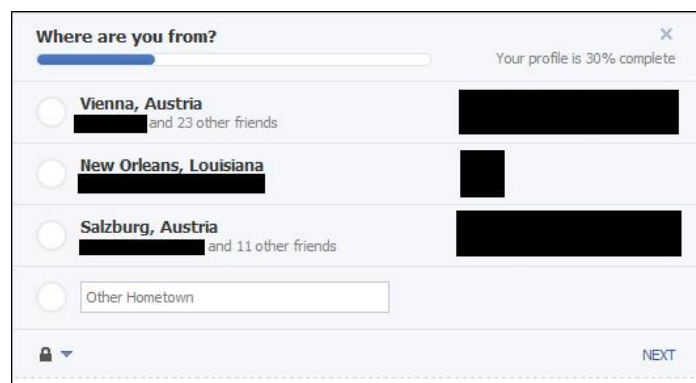
This allows for profiling on people that have never really shared anything on facebook.com, or are not even a member of the platform (as pointed out in the initial complaint). In other cases, data that the user did not knowingly share or is not visible is processed in a way that a profile can be derived that is much bigger than what is visible for the user – which is why I consequently called this phenomenon “shadow profiles”.

The problem of this is the total loss of control by the data subject. This is the result of a mix of data that was initially collected for a variety of purposes, no possibility to give a “specific” consent and not even a way to amend, remove or “opt-out” of such processing. Just about every principle of data protection law is thereby violated by such processing. On the next pages I want to name a couple of examples. At the same time this is likely just a small excerpt of the phenomenon.

→ **F18: FB-I is analyzing information across the profiles and data categories. In addition FB-I is collecting other data without the knowledge of the user and “adds” them to the data that users shared voluntarily.**

Example 1: Suggested Hometown

A very plastic example of the results of such analysis is a recent function FB-I has introduced to suggest additional information about a user. This function seems to analyze patterns among users’ friends to then suggest that a user might e.g. live in a certain place or was working at a certain company. Interestingly the system is generating very reasonable results:



Screenshot: Facebook is generating last workplaces through “big data” with data from me

In the first case FB-I is calculating my hometown. I am born in Salzburg and moved to Vienne when I was 18 years old. This I have not shared with FB-I (my hometown was previously set to “Salzburg” and my

current city was previously set to “Vienna”) but it apparently generates this information via analysis my network of friends. There is no control by the user over such analytical process and no way of “avoiding” such processing – unless users do not have friends at all.

However FB-I seems to go further than only counting friends. The suggestion that I might be from “New Orleans” seems to be absurd given the fact that only one (!) friend of my friends has entered this place has his hometown. It would be totally unreasonable that I FB-I would suggest this as my hometown given that I got e.g. 5 friends from “Linz” and “Graz”, 4 friends from “Innsbruck” or 3 Friends from “Klagenfurt”. However FB-I is constantly suggesting that I might be from “New Orleans”.

After reviewing other data I could find however that I mentioned “New Orleans” three times in deleted messages, three times in undeleted messages and I was the title of a photo album when I was meeting with my American host family in “New Orleans”.

In all cases “New Orleans” was associated with the word “family” (in “host family”) as I was organizing parts of the trip through facebook.com. It seems logical that FB-I’s algorithms assume that I would meet with my “family” in my “home town” and are therefore suggesting “New Orleans”.

Other Suggestions

The image shows two side-by-side screenshots of Facebook's profile completion interface. Both prompts have a progress bar at the top indicating 'Your profile is 30% complete' and a 'NEXT' button at the bottom right.

The left prompt is titled 'Where did you go to college?'. It lists three suggestions, each with a radio button and a link to 'and [number] other friends':

- ☐ University of Vienna and 49 other friends
- ☐ Vienna University of Economics and Business and 12 other friends
- ☐ Santa Clara University School of Law and 3 other friends

Below these is a text input field labeled 'Other College or University Name'.

The right prompt is titled 'Do you work at any of these places?'. It lists three suggestions, each with a radio button and a link to 'and [number] other friends':

- ☐ AFS Intercultural Programs and 15 other friends
- ☐ Rotes Kreuz Salzburg and [redacted] other friends
- ☐ AFS Malaysia and 3 other friends

Below these is a text input field labeled 'Other Company'.

In similar cases I was suggested to have gone to “Santa Clara University”, despite 5 friends of mine being at Uni Graz, which would be more reasonable to suggest. However I have little contact with them and I never used “Uni Graz” in messages while I mentioned “Santa Clara University” in 8 undeleted and 7 deleted messages. In fact I was studying at Santa Clara University.

The same is true for my work as a volunteer at “AFS” and as a community servant at the “Red Cross” in Salzburg. I was in Malaysia for one month on a trip through “AFS”. While I am currently not sharing any association with these organizations FB-I was apparently analyzing my friends’ data to figure this out.

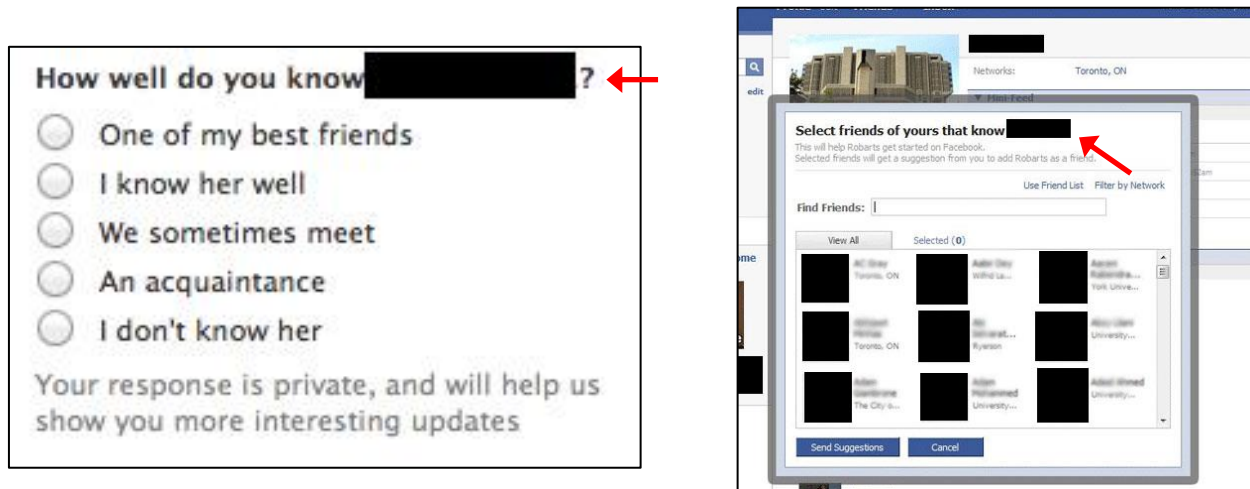
➔ ***F19: FB-I is analyzing different information across the profiles the user and his friends to figure out more about a person than this person is actively sharing with FB-I. Such information is generally not visible and not editable or removable by the user. The data adds to what I initially called “shadow profiles”.***

Example 2: Friend Suggestions

Another use of the “network” data by FB-I is (as previously explained) the “friend suggestion” feature. In this respect I want to add that I now had to find that even “hidden” friend lists can be extracted this way: If a new account is making friends with another person, then the entire friend list of this other users is shown as “friend suggestions” – even if the other user has set his friend list to “only me”.

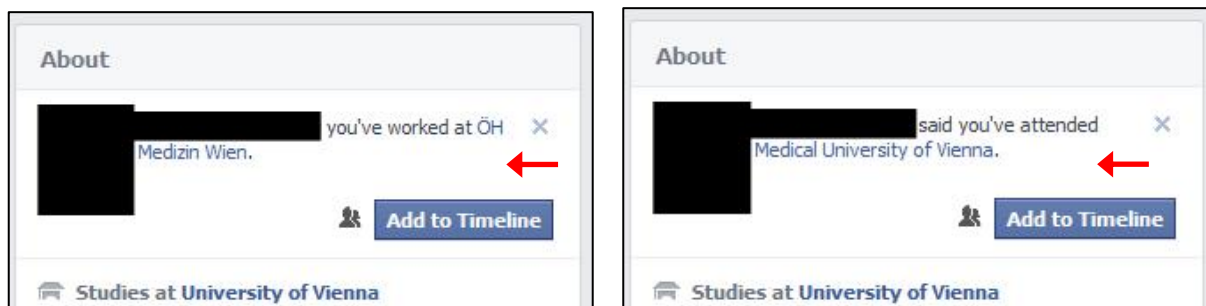
Example 3: “Spying” on your Friends

In my initial complaint I was pointing out that FB-I is e.g. using other people’s address books to figure out information about non-users or users that did not indicate a relationship to that person. In addition to that I now had to find many other cases in which FB-I is following this tactics. The most basic versions are that FB-I is asking “friends” rather blankly about other “friends” – or people they are adding as friends:



Screenshots: “Friends” are asked about others. Even when they only made a “friend request”

In another example FB-I is now also asking users who of their friends are also working or studying at the same institution that they are. FB-I is actively promoting that users are “spying” on each other and turn over information about each other. This is sometimes “surfaced” by a suggestion to “add” this information:



Screenshots: “Friends” have shared work and educational information about a user – FB-I is using the information.

In another (widely reported) case FB-I has even asked users if the names of their friends are correct – or if they have used a wrong name. FB-I has said in the message that the information will not lead to any problems for the person using false names.



The screenshot shows a Facebook survey interface. At the top, a blue header bar contains the text "Help Us Make Facebook Better". Below this, a message reads: "Please help us understand how people are using Facebook. Your response is anonymous and won't affect your friend's account." A red arrow points to the word "people" in this message. The survey question is "Is this your friend's real name?". To the left of the question is a blacked-out profile picture and a blacked-out name. Below the name, it says "Lives in [redacted] Oregon". To the right of the question are four radio button options: "Yes", "No", "I don't know this person.", and "I don't want to answer." The last option is selected. At the bottom left is a link for "Name policy", and at the bottom right is a blue "Submit" button.

Screenshots: "Friends" are asked if the names of users are correct.

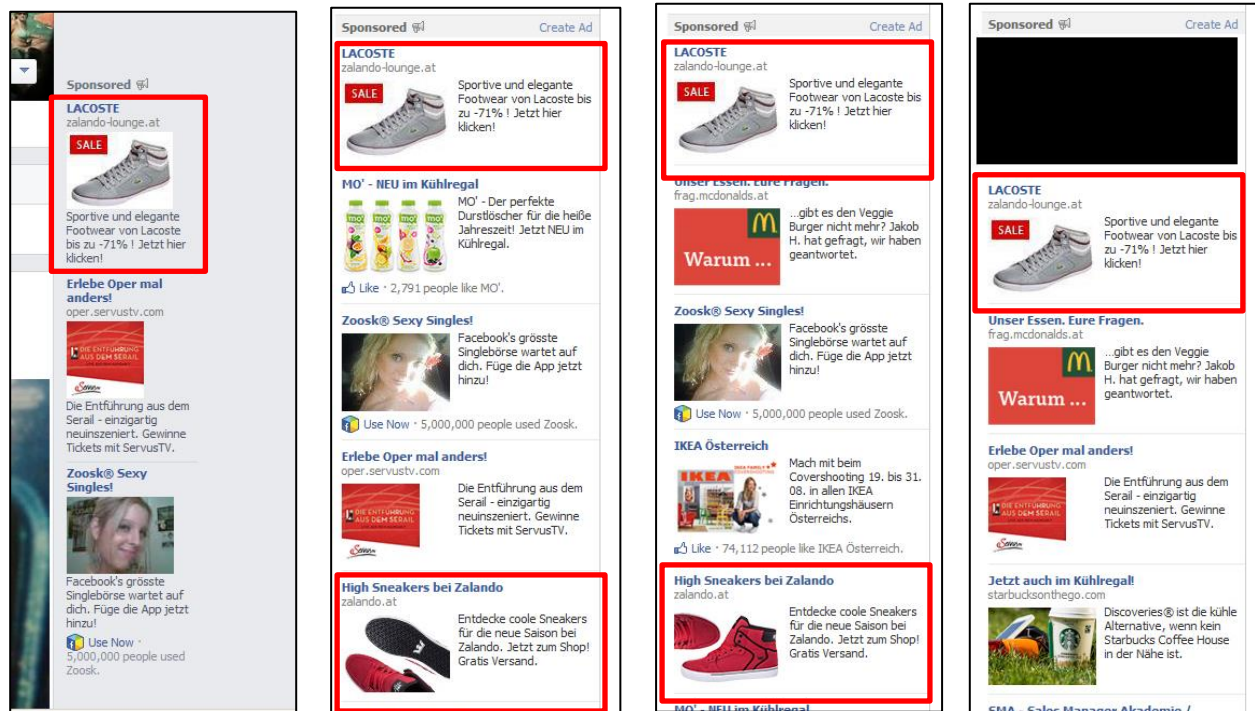
However we received a large number of emails from people that were blocked from "facebook.com" and used a false name during this time, which indicated that FB-I was using this information to block users that did not provide their real name. This indicates that FB-I has collected this information under misrepresentation of the facts.

All the data above is never included in the "download tool" and cannot be seen by the user. Users cannot edit it, correct it or remove it in any way. There is no form of specific consent by the user.

➔ ***F22: FB-I is collecting data about users via other users. This data is held in the background without any specific consent by users, without access to the data, without options to edit or remove such information and adds to what I initially called "shadow profiles".***

Example 4: Facebook Exchange (FBX), Re-Targeting and “Tracking”

Another form of “shadow data” is data FB-I is getting from other companies about users. Such as data it gets through “retargeting” under the “Facebook Exchange” system. After I have found that the German online shoe retailer “Zalando” is taking part in this system I made a visit to the webpage of “Zalando” and started the payment process for a pair of Adidas sneakers. I never saw advertisements from “Zalando” on facebook.com. The next time I was loading Facebook I got “Zalando” advertisements all over Facebook only featuring Adidas and Lacoste sneakers:



Screenshots: Advertisement on Facebook after not finishing a purchase of sneakers on “zalando.com”

The “targeting” stayed for days even after I deleted all cookies from my browser or used another browser. This means that the information is stored with my profile at FB-I.

When I downloaded my personal data (via the “download tool”) there was no related information stored with my profile. Only the fact that I clicked one of the Ads was stored with my profile. This however only said “LACOSTE (Clicked Ad), Thursday, August 22, 2013 at 6:22pm UTC+02”. There was however no information that would in any way relate to “zalando.com” that is the company all advertisements relate to.

➔ **F20: FB-I is collecting data about users from third parties for “re-targeting”. This data is held in the background without any specific consent by users, without access to the data, without options to edit or remove such information and adds to what I initially called “shadow profiles”.**

In a recent interview the product manager of FB-I is also talking about an option to track users on other pages without the use of cookies (and without any chance to “opt out” through deletion of cookies). The person from FB-I is explicitly saying that this form of tracking is independent from the user being logged in or not and is therefore not in any way comparable to the systems the DPC has evaluated in its initial “audit” in 2011 and 2012.

AdExchanger: What is Facebook doing in cross-device attribution?

DAVID BASER: Just as with all other conversion measurement systems out there, we provide advertisers with a snippet of code for their websites. That snippet generates a ping when a user takes a desired action. The key difference is that other conversion measurement systems rely on dropping cookies on the users when they see or click on the ad. We understand who the user is regardless of whether they're logged into Facebook on the app or on the mobile phone.

When that ping comes back from a user taking an action on the customer's website, we associate that back to the user ID without relying on a cookie ID.

Once we have this system based on user IDs and not based on cookies, we can use it to have consistent attribution across web, mobile and even multi-browser on the desktop.

If an ad shown on the mobile newsfeed says "Check out our website" and [the site] is not optimized for mobile, even if a user goes next day or next week, an attribution will be assigned regardless of the where ad is shown.

(Link: <http://www.adexchanger.com/social-media/product-manager-david-baser-on-facebooks-attribution-roadmap/>)

➔ **F21: FB-I can “tack” users across other pages – independent from cookie settings and log in status.**

Example 5: Cooperation with “Data Brokers”

In February 2013 Facebook announced (<https://www.facebook-studio.com/news/item/new-ways-to-reach-the-right-audience>) that advertisers can now also use consumer data stored by big data brokers when targeting advertisements towards users of facebook.com. In essence FB-I is getting a number of hashed individual identifiers it runs against its own users. The resulting list of users is then targeted. Through this form of advertisement FB-I can add “real world data” to the existing profiles of users.

Despite the fact that data is said to be “hashed” the information “Susan Peterson is expecting a baby” is still transferred to FB-I. By “hashing” identifiers (in this case likely the email of a user) FB-I is only lowering the amount of information exchanged, but is not bypassing the fact that information is exchanged without the users’ consent, information or possibility for removal of the data. Further information can also be found here: <https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads>

In April 2013 this program was expended to “small” advertisers. In a blog post (<https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature>) FB-I noted:

“Today we’re launching partner categories, a new way to target ads to more categories of people. For example, a local car dealership can now show ads to people who are likely in the market for a new car who live near their dealership. To date, advertisers have been able to show ads to people based on their expressed interests on Facebook. Now with partner categories, they can also show ads to people on Facebook based on the products and brands they buy across both desktop and mobile. Partner categories uses data from select third parties including Acxiom, Datalogix, and Epsilon.”

The companies named in this blog post are among the biggest data dealers in the world. Acxiom was e.g. said to hold consumer profiles of more than 500 million people in 2012 with about 1.500 data points per person (figures by the New York Times).

➔ **F23: FB-I substituting its own data with data collected from “data brokers” without any information to the users, without means of accessing this data, without specific consent of the data subject and not even with an option to “opt-out”.**

Example 6: Publicly available Data / Wikipedia

In another case I was able to see that FB-I is combining data from my profile with other, publicly available data. Through the “download tool” FB-I is giving a short list of “Ad Topics” it thinks people are interested. Most of them just seem to be based on pages a user “likes”.

However in my data set FB-I was listing (among other obscure things) that I would be interested in “electronic viewfinders” – something I had to search online to know what it is. There is no connection whatsoever between me and “electronic viewfinders”. Interestingly the “electronic viewfinder” was also in the “Ad topics” list of other colleagues of “europe-v-facebook.org”. After reading the Wikipedia article on “electronic viewfinders” I was able to see the connection: “Electronic viewfinders” are abbreviated as “EVF” on Wikipedia – the name of the Facebook page of “europe-v-facebook.org”.

Similarly FB-I thought I was interested in “Arabesque (Islamic Art)” – based on the fact that I “liked” the middle east correspondent of the Austrian Broadcaster ORF named Karim El-Gawhary Arabesken. In another case FB-I thought I was interested in “Kobuk, Alaska” – a town with 150 inhabitants. This seems to be based on “liking” the Austrian media watchdog page “Kobuk”.

Interestingly the solution of the misunderstanding could be found by consulting Wikipedia. It seems like FB-I is mainly relying on them to substitute information.

➔ **F24: FB-I substituting its own data with data collected from the internet or Wikipedia.**

➔ **F25: The systems used by FB-I are producing incorrect and obscure results.**

Information provided by FB-I

The latest version of FB-I's privacy policy is in some way touching upon the fact that this form of gathering from third parties is happening. In the section that explains the gathering of data FB-I explains:

"Information others share about you

We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group. When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts.

Other information we receive about you

We also receive other types of information about you:

- (...)
- *Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads"*

However there is no more specific information to data subjects. The wording "*information about you from your friends and others*" allows basically anyone in the world to submit any kind of personal data to FB-I. In addition FB-I says the following about the combination of data that it gathered::

"We also put together data from the information we already have about you and your friends. For example, we may put together data about you to determine which friends we should show you in your News Feed or suggest you tag in the photos you post. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you that you might be interested in. We may also put together data about you to serve you ads that might be more relevant to you."

From this one could derive that for the purpose of advertisement data is only put together about the individual person (see "*data about you*" – not e.g. "*about you and others*"). However in a later section of the privacy policy FB-I goes on to say:

"We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use."

This would again mean that FB-I allows itself to use any data, for any purpose and in relation to any third party as long as all this happens "in connection with the services and features" it provides to anyone in the world today and in the future.

➔ ***F26: The wording used by FB-I is the most unspecific and ambiguous wording a controller could think of. There is no way this wording could be the basis of an "unambiguous, specific and informed consent".***

Summary of additional Facts

FB-I is today generating data on users that go far beyond what users have voluntarily shared. In this document I could only refer to some situations, which can in no way be seen as complete. Further investigations are necessary. However two facts are apparent from the available evidence:

First of all FB-I is **collecting data via third parties** (e.g. users, advertisers, Wikipedia or data brokers) without any form of information or consent by the data subject and without any respect of the principles of data protection (section 2(1) DPA and Article 6 of Directive 95/46/EC). Most of this data is invisible and only “surfaces” in certain situations. None of the data is included in the “download tool” or any other form of transparent information by FB-I.

In addition FB-I is then analyzing data across user profiles, data categories and data sources. This form of **“big data” analysis** is making it impossible for a user to rectify, opt-out or limit the amount of information FB-I is able to get about him or her. Just the fact that a data subject is friends with a number or people leads to assumptions by FB-I. The concrete use of data is not visible for a user, only in some cases one can assume which data has led to a certain result. An average data subject is unable to understand, consent or object to such form of processing.

- ➔ ***F27: FB-I is in many ways collecting data from third parties to supplement data users have voluntarily shared and thereby created “shadow profiles” of users. Data subjects have no way to know or controlling this data gathering.***
- ➔ ***F28: FB-I is analyzing data across profiles, data categories, data sources and processing purposes. This “big data” analytics makes it impossible for users to know or control their data.***

C. Reaction by FB-I and the DPC:

In the section on advertisement in the report from December 2011, FB-I only seems to mention the most basic possibilities to target ads. There is no word on more sophisticated functions as described above, even though such techniques are “state of the art” and are knowingly deployed by most internet giants. It seems like FB-I has only disclosed the types of data processing that are very obvious and reasonable. When considering the exact wording of such statements, it becomes clear that they are all written in a way which also allows for other processing:

“For example, FB-I stated that if a user mentioned a car in a status update and also “liked” something related to cars, FB-I might target ads to the user at a potential car buyer.” (Report, Page 45)

This does not say, that FB-I does not use other, less obvious, information to target ads, promote their service or suggest “friends”. In the end this statement is only “legal talk” without expressly saying which factors are and are not playing a role in advertisement and analytics. Overall there is a huge disagreement between what FB-I is claiming towards the advertisement industry and what it is claiming in respect to the DPC. I was only able to name a few of these discrepancies.

The audit and the technical report cover so far only the small fraction of this form of processing that was deployed by FB-I to “friend suggestion”, but did not elaborate the overall problem of “shadow profiles” and data processing by FB-I that is not solely based on the information that users have deliberately shared on facebook.com. My complaint 02 clearly names the “friend suggests” as only one of many possible results of these extensive profiles.

At the same time much of the evidence submitted above have also only been available within the past months, which might explain to a certain extent why the DPC was unable to look at this issue in more detail. My initial complaint was also only giving a “hint” in this direction but was not as explicit as other complaints. I am therefore happy that the DPC was explicitly asking me to “amend” my complaints.

- ➔ ***F29: There is nothing in the “audit” reports that would in any way indicate that the facts relied in the initial complaint and supplemented above would in any way be incorrect. FB-I and the DPC have “bypassed” the issue.***
- ➔ ***R21: I hereby ask the DPC to fully investigate the issue, as explained above. It is necessary that the DPC is using its enforcement powers to search for all cases where FB-I is collecting user data through third parties. In addition I hereby ask the DPC to use its powers to establish the ways and forms of analysis across profiles, categories and sources by FB-I.***

D. Legal Consequences:

WP 203 by the Article 29 Working Party:

The Article 29 Working Party has recently published WP 203 dealing with “purpose limitation”. In this opinion the Working Party is also dealing with the phenomenon of “big data” which seems relevant concerning this complaint. In summary the Working Party has held that

“[t]he purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.” (WP 203, page 15)

The main issue seems to be that FB-I has to name the specific purpose for each processing operation. Currently FB-I is only referring to its privacy policy which is in no way meeting the requirements of the law concerning “shadow profiles” or “big data” analytics. As FB-I is using all data, from all sources for any purpose that relates to its business there is in essence no limitation whatsoever:

“We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”

The only thing FB-I's wording does not allow is processing of data outside of the scope of its business and to share it with entities it does not have a relationship to. However as soon as FB-I is engaging in such activity it would be covered by the wording of FB-I's policy.

There is no way that a data subject can consequently know *"what kind of processing is and is not included within the specified purpose"*. As FB-I is factually allowing itself to use any data for any purpose FB-I does not *"allow that compliance with the law can be assessed"*.

The Article 29 Working Party is even allowing for "layered notices" or "sub-purposes" for controllers:

"It is generally possible to break a 'purpose' down into a number of sub-purposes.

- For example, processing an individual's claim for a social benefit could be 'broken down' into verifying his or her identity, carrying out various eligibility checks, checking other benefit agencies' records, etc.

- The concept of an overall purpose, under whose umbrella a number of separate processing operations take place, can be useful. This concept can be used, for example, when providing a layered notice to the data subject. More general information can be provided in the first instance about the 'overall purpose', which can be complemented with further information. Breaking down the purposes is also necessary for the controller and those processing data on its behalf in order to apply the necessary data protection safeguards." (WP 203, page 53)

However FB-I has not even responded to "access requests" with a more "specific" purpose, but only referred to its privacy policy. Overall FB-I seems to perfectly fit into what the Article 29 Working Party was describing by this example:

"The above example can be contrasted with that of a large retail company selling goods via a website all across Europe and using complex analytics to inform personalised offers and targeted advertisements. In this case, the purposes must be specified in a much more detailed and comprehensive way, including, among other things, 'the way in which' personal data are processed. The decisional criteria used for customer profiling must also be disclosed."

➔ **F30: The "specific"-test for the purpose FB-I is delivering is absolutely not met.**

The Working Party is further saying that data must be collected for an "explicit" purpose. When elaborating about this requirement the Working Party was finding that:

"The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. What is meant must be clear and should leave no doubt or difficulty in understanding." (WP 203, page 17)

The wording by FB-I as outlined above can in no way meet this test. FB-I is using the vaguest wording possible when just talking about "others" and "other third parties" that they "may" collect data and only specify the purpose when saying the data is used *"in connection with the service"*. The very general statements are usually just accompanied by "examples" that do not limit FB-I in any way as they are just one case that falls under the general rule.

➔ **F31: The "explicit"-test for the purpose FB-I is delivering is absolutely not met.**

Further Use of Data for a Compatible Purpose

As outlined above FB-I is combining data it is processing on behalf of the user (who is the controller) with data from other users, third parties (e.g. data brokers, advertisers) and from the public domain and is then cross analyzing all this information. Every step in itself is a form of “processing” of such data and constitutes “**further processing**” outside of the primary purpose. Most of the data does not have a primary purpose that is in any way compatible with “big data” analytics (if I e.g. post on a friends’ page the purpose is communication and this is in no way compatible with “big data” analytics).

The details of FB-I’s position on the purposes are unclear since I was not provided with the necessary files and FB-I is not responding properly to access requests and does not fulfill its duty to give proper information. The DPC will have to draw a line and may be following the work paper on this matter:

“While the publicly specified purpose is the main indicator of what the data processing will actually aim at, it is not an absolute reference: where the purposes are specified inconsistently or the specified purposes do not correspond to reality (for instance in case of a misleading data protection notice), all factual elements, as well as the common understanding and reasonable expectations of the data subjects based on such facts, shall be taken into account to determine the actual purposes.” (WP 203, page 19)

In order to determine a rough separation into different purposes I am referring to the section above about the controller issue, which can also be utilized in this respect and leads to reasonable results. When data that is only held as a “processor” is further used as a controller, there is a clear line when the purpose has changed. When I am e.g. posting on my page the purpose is that my friends see what I posted there. It is surely not the purpose of such a posting that I want to be subject to “big data” analytics. If a friend of mine now “likes” this post the purpose is again that I know he likes my post (any maybe feel a little more loved by the world). In any event the purpose is not that “big data” analytics is now targeting this friend with advertisement. The Article 29 Working Party has outlined this rather clearly when saying:

“...any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered ‘further processing’ and must thus meet the requirement of compatibility.” (WP 203, page 21)

- ➔ **F32: FB-I does not specify the purposes in any way that is compliant with the law. Therefore the DPC will have to assess this matter based on factual elements and a common understanding.**
- ➔ **F33: FB-I’s use of profile data for “shadow profiles” (or “big data analytics”) constitutes “further processing” within the meaning of the law.**
- ➔ **R22: I hereby ask the DPC to get a statement from FB-I about the purpose(s) and gather all evidence and arguments necessary to bring light into this issue. If FB-I is not submitting any substantial information I hereby ask the DPC to map out what form of processing is done for which purpose, form an opinion on when there is a change in purpose and inform me about his findings.**

After finding that FB-I is “further processing” certain data one must assess if this further processing is “**compatible**” with the initial purpose. In the case of FB-I one must separate between different kinds and sources of data: While it seems very unreasonable to ask friends about the “real names” of user, or it seems very unexpected that FB-I is adding information from “data brokers” or gathers information from the “internet” and connects them with data on users, it might be more obvious to use data that was voluntarily and publicly shared by a data subject.

Surely this question can clearly not be answered easily. Compared to cases where it is impossible to deliver a service without further use of data (e.g. forwarding of shipment data to the postal service when ordering a product online) there is no direct need for FB-I to further process such data. FB-I could also just have normal advertisement, or “targeting” based on data that is not related to a person. The question whether a purpose is “compatible” is a multi-factor test. The Working Party has tried to name “key factors” when assessing such “compatibility” and named the following factors in its analysis:

- a) the relationship between the purposes for which the data have been collected and the purposes of further processing*
- b) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use*
- c) the nature of the data and the impact of the further processing on the data subjects*
- d) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects (WP 203, pages 23 to 26)*

The analysis has to be done after establishing every data category, every source and the specific purpose of the use of each data category. However the Working Group has summarized its general view on “big data” processing for targeting of individual data subjects in the following section:

“The second potential scenario is when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform ‘measures or decisions’ that are taken with regard to those customers. In these cases, free, specific, informed and unambiguous ‘opt-in’ consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.” (WP 203, page 46)

The Working Party goes on to interpret the conditions for such consent to be “informed”:

“For the consent to be informed, and to ensure transparency, data subjects/consumers should be given access to their ‘profiles’, as well as to the logic of the decision-making (algorithm) that led to the development of the profile. In other words: organisations should disclose their decisional criteria. This is a crucial safeguard and all the more important in the world of big data. More often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern. Further, the source of the data that led to the creation of the profile should also be disclosed.” (WP 203, page 47)

- ➔ **F34: It is highly questionable if FB-I can show that there is a “compatible use” of this data.**
- ➔ **F35: FB-I is in no way getting a valid consent for such “further processing” that would meet the requirements set out by the Article 29 Working Party.**

Summary of the Legal Consequences

The legal consequences of the previously described phenomenon of “shadow profiles” are not fully fitting the additional facts I have submitted. Therefore I would like to replace them with the following claims (all are based on the claims on the original complaint):

1. There is no transparent, specific and clear notice that “shadow profiles” are held, to what extent they are used, which data is gathered, what sources used and that “big data” analytics is conducted by FB-I. Information is also unclear and misleading which breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.
 2. There is no information in FB-I’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) DPA.
 3. FB-I can in no way secure that these shadow profiles are accurate, kept up to date and complete as it allows anyone to add data but does in most cases not disclose the functions or results of such processing. Where data is disclosed (see e.g. my “ad topics”) they show clearly that the systems produce false and obscure data. There is no way to amend, change or rectify this information. This breaches section 2(1)(b) DPA and Article 6(1)(d) of Directive 95/46/EC.
 4. Data is used across purposes, data subjects and sources. There is no specified, explicit and legitimate purpose as required by law. In fact FB-I uses any data for any purpose without any limitation. This is a breach of section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.
 5. The “further processing” of this data does not seem to be “compatible” with the initial purpose in most cases which constitutes a breach of 2(1)(c)(ii) DPA and Article 6(1)(c) of Directive 95/46/EC.
 6. The data is no longer relevant for the initial purpose of the processing and seems to be also excessive (any data, from anyone, for any purpose and shared with anyone), which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.
 7. The processing of the data seems to be longer than necessary to fulfill the purpose it was collected for. This constitutes a breach of section 2(1)(c)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.
 8. The data subjects have never given a specific, informed and unambiguous consent to the processing of the information gathered by Facebook Ireland. There are general provisions in the privacy policy, but the user has no way of finding out exactly which information is gathered. Data subjects have not even any way to know or react to this form of processing. Non-users have not even consented to the privacy policy of Facebook Ireland. This means that there has never been a specific, informed and unambiguous consent as necessary under section 2A(1)(a) DPA or Article 7(a) of Directive 95/46/EC.
- ➔ ***R23: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed in my amended complaint and is also continuing to do so. I ask to prevent such processing.***
- ➔ ***R24: If the DPC departs from the common understanding of the Article 29 Working Party as outlined above I hereby ask him to explain this and say why he does so.***

6. Complaint 03 “Tagging”

A. Facts described in the original Complaint:

The Facebook Platform gives users the possibility to “tag” another user (“friends”) in photos. This means that the photo, which is not really machine-readable with today’s technologies, is becoming easily machine-readable. Tagged photos are also displayed on the data subjects Facebook page and the “news feed” which is the start page that all “friends” of the user will see when logging onto Facebook. This news feed is the information of friends that was aggregated by Facebook.

Data subjects do not have any possibility to prevent other “friends” from tagging them in pictures, other than not having friends at all. The tag is fully active before the data subject even knows about its existence. There is no functionality that prevents unwanted tags in pictures. The only option the data subjects are given is to remove tags, as soon as it sees it, but this may be too late.

In practice this means that the data subject may be tagged in a picture where it can be seen drunk, cheating on its partner/spouse, naked or any other problematic situation. This picture will be automatically distributed by Facebook Ireland to all “friends” of the data subject. When using the standard settings of the facebook platform, all internet users are able to see the data subject’s pictures. The only option the data subject has is to remove the tag after all this has already happened (opt-out).

To prevent other users from “tagging” the data subject in the same picture again, the tag that got “removed” by the data subject is still saved on the facebook platform. This can be seen by the data field “active” that is used by Facebook Ireland (if the the tag would be removed there would be no need for an “active/inactive” option, see attachment 03) and by the prompt that the user is getting if he tries to tag the data subject a second time (see attachment 04).

This means that the user can in fact never remove the tag from the facebook platform. All tags are kept by Facebook Ireland, even if the user “removed” the tag.

In section 5.9. of Facebook Ireland’s terms they are saying: “You will not tag users (...) without their consent” (see attachment 01). In the daily practice this provision is not known to the users at all. In my personal experience after 3 years of using the Facebook platform, there has never been another user that asked me for my permission before I was tagged in a picture.

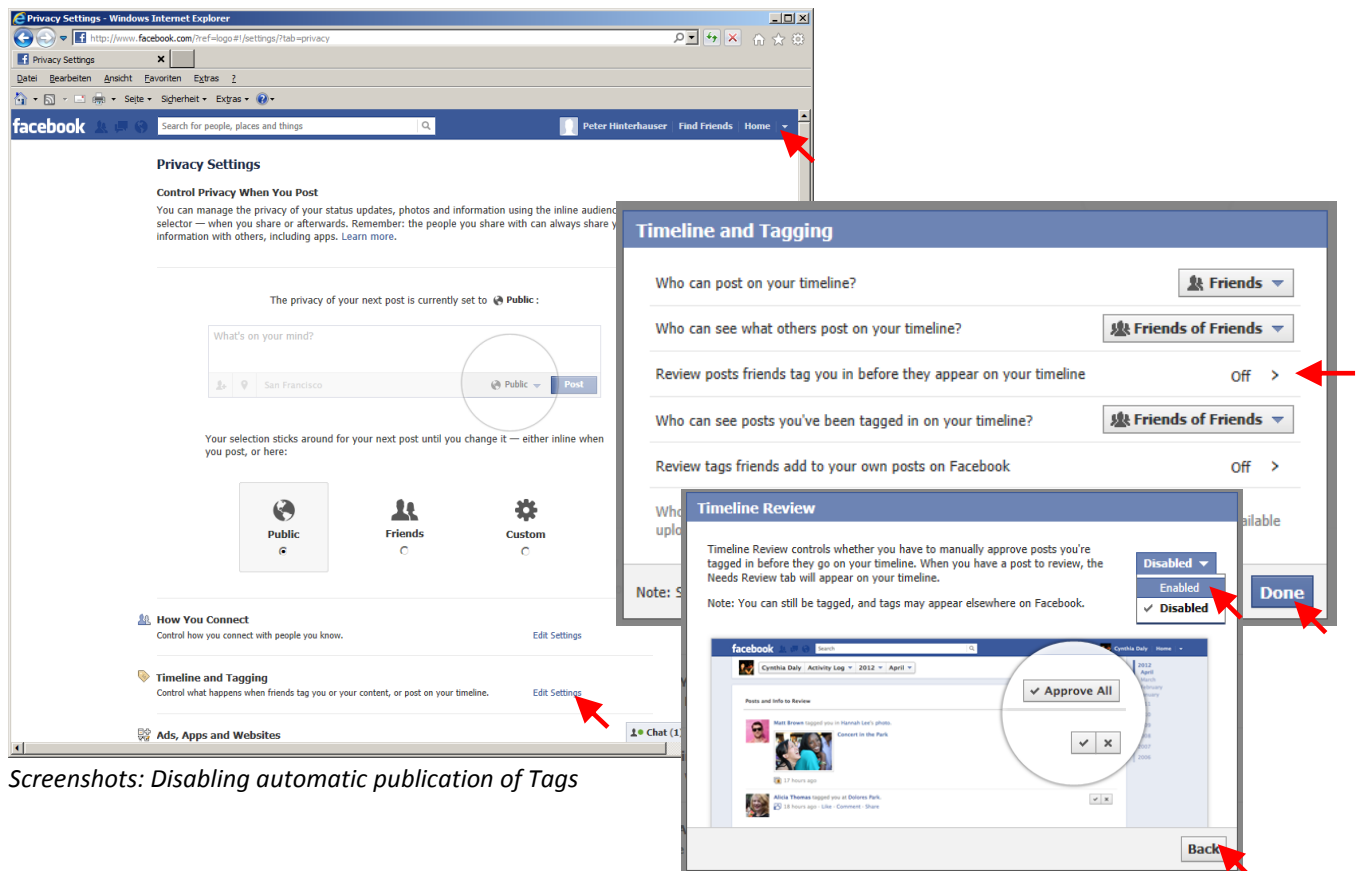
I do think that this (unknown) provision is not sufficient to make Facebook Ireland a bona fide user of this information that is delivered by users. Different data protection authorities in the EU have ruled that a mere legal obligation or protection is not sufficient if it is not enforced in practice.

In summary Facebook Ireland is processing personal data (tags) without the specific consent of the user. General provisions in the privacy policy do not constitute a specific consent. The user knows that some picture might be tagged by some user, but this information is in no way substituting a specific consent. There is a major difference in the processing of different kinds of pictures. Facebook Ireland is not tagging the users itself, but it is using the personal data that is obtained without the specific consent of the user for its own purposes (e.g. aggregating the news feed, analytics about users).

B. Additional Facts:

Changes by Facebook

Following my complaints FB- I has introduced the option to preapprove “tags” before they are publically shown. At the same time this is just a first step in the right direction, since users have to actively opt-out from automatic publication of tags that other users can place at any time. It takes many steps to deactivate the automatic tagging mechanism (8 clicks). Compared to the other options in the relevant pop-up FB-I requires users to go down one more level into the menu, by having a second pop-up that is only accessible through a text link, instead of a button (like the rest of the option). The wording is also confusing, since users have to choose “enabled” to prevent the automatic publication of tags.



Screenshots: Disabling automatic publication of Tags

This change to the previous system only changes the initial **visibility** of tags (in pictures or postings). It does not change the tagging mechanism itself. It does also not change the removal of tags. FB-I still keeps all “removed” tags – so a user cannot get rid of the association with a picture.

➔ **F36: The new system only allows an “opt-out” from automatic publication of tags. There is no change in the rest of the process. Data is still collected without the specific consent from a data subject and it is still impossible to remove tags (details on the removal see “Complaint 11”).**

Further Use by Facebook

Since I have filed the original complaints I was also able to collect evidence that FB-I is using unapproved “tags” to analyse the behavior of data subjects. I was tagged at specific place (“check-ins”) repeatedly by a friend (despite the fact that I have informed him that I do not want to be tagged).

I never approved tags but clicked “hide” whenever asked (FB-I offers the options “Add to Timeline” and “Hide”). Despite the fact that I have not approved them FB-I has used them when suggesting that I should “rate” the following places in Vienna:



Screenshot: FB-I is using “hidden” tags to suggest that I should rate places I have visited.

The places that were suggested by FB-I are mainly places I regularly visit. At the same time they match exactly the places I was checked in by my friend (three are marked as an example, all others are also corresponding with a “tag”). FB-I is still using such information for its own purposes.

➔ **F37: FB-I is using unapproved tags by third parties for its own purposes and targeting. There is no form of consent to such use.**

C. Reaction by FB-I and the DPC:

According to the DPC's report the main arguments by FB-I were the following:

"They always receive notifications when they have been tagged and they have always had the ability to un-tag themselves. Tagging enables users to get immediately informed when their friends mention them in a post or a photo. It gives them more control since they can react positively, express their discomfort and ask for the removal of the content if they wish or simply respond to an assertion in which they're mentioned."

"Facebook has (...) added the ability for users to preapprove tags before they appear on their Timelines (formerly, profiles). Thus, Facebook ensures 1) notice of all tags to users; 2) the ability to require prior notice of all tags; 3) the ability to un-tag; and 4) the ability to simply block it from appearing on the user's own Timeline. Facebook firmly believes that it has struck the right balance in terms of product development and user control." (both: Frist Report, page 127).

The DPC has said the following in its first "audit" report:

"If (...) a member tags a picture or a comment, post etc with a tag identifying a friend, an association with the friend is made and they are sent a notification of the tag with an ability to remove it. (...) In the Retention section of this report we have outlined the measures that will be introduced to allow a user to delete such tags subsequently if they wish to do so. For those members who do not wish to be tagged at all, it is the case that at present there is no ability for them to express their preferences. (...) While preventing the tagging of yourself would mean that you would be less likely to become aware of a picture, post or comment in which you are referenced, there does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it." (First Report, page 126)

The DPC has changed its position from the first "report" in the second "review". While in the first report it has said that *"there does not appear to be a compelling case as to why a member cannot decide to prevent tagging"*, it has changed its position without any material argument that was any new:

"Taking account of the various tools available to users to manage Tags and to delete them if they so wish I am not requiring an ability to prevent Tagging at this time." (Review, page 47)

Only some numbers from the United States (!) that indicate that "only" 22% remove picture tags seemed to be new. This does however not lead to any assumption that the law would not apply in this case.

The reports are not covering other issues brought up in my initial complaint, especially the question how there could possibly be an *informed* and *specific* consent by the data subject to the postings, if the data subject does not even know which kind of picture or posting he/she got connected to, was not covered.

The law does not allow to process data based on "consent", if there is no affirmative action by the data subject. The "audit procedure" was also missing another point: The law applies to "visible" and but also "invisible" data. Even when people remove the tags, FB-I still keeps the information. It is just not visible anymore, but can still be used to track users or serve "relevant ads". Even just the fact that the information is kept constitutes "processing" of personal data.

➔ **F38: FB-I and the DPC highlighted the function as of "tags" as information to the data subject, the ability to remove the visibility of "tags" and statistical numbers of "un-tagging" in the US. Neither the DPC nor FB-I have commented on the core problem of "consent" and other issues.**

D. Amended Statement concerning Legal Consequences:

FB-I is still collecting data via third parties without any specific, unambiguous or informed consent by the individual data subject. The “audit” and the arguments by FB-I have in no way covered the issues brought up in the complaint. As the original complaint has mixed up the removal of “tags” (see Complaint 11) I would like to amend this complaint and replace the claims with the following statement:

1. There is no specific and informed consent by the data subject for the individual tag (opt-in). There is a big difference in what information a user is associated with, which makes it impossible to give a general consent to “any information” that is submitted by “any friend”. This constitutes a breach of section 2A DPA and Article 7(a) of Directive 95/46/EC and makes any further processing illegitimate.
2. Data is obtained through other users without any chance to intervene, object or remove it which breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.
3. FB-I can in no way secure that these “tags” are accurate, kept up to date and complete as they cannot be seen, changed or amended. At the same time any friend can “tag” someone at any time. This breaches section 2(1)(b) DPA and Article 6(1)(d) of Directive 95/46/EC.
4. Data is initially shared to e.g. mark someone in a picture or at a location. FB-I is using this information for other functions such as the “rating” function noted above. “Further processing” of this data is not “compatible” with the initial purpose which constitutes a breach of 2(1)(c)(ii) DPA and Article 6(1)(b) of Directive 95/46/EC.
5. Processing this data is excessive, inadequate and not relevant for the purpose it was initially obtained for which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.

Currently I am only aware of one solution which I would understand to be compliant with the law. This solution is by the way the standard procedure with “invitations” or “adding” people in just about all other systems I know of:

Step 1: A third party can establish a link between a data subject and an object (invitation).

This link stays inactive until there is an action by the data subject.

Step 2: The user gets a notice to “accept” or “remove” it.

Step 3: Removed links are deleted, users may get the option to “stay disconnected” (the removal is then stored).

Accepted links are turning into a visible link (e.g. a tag, group membership or RSVP) and may be processed further by FB-I (e.g. for serving ads).

Additional systems like limiting the users that can establish links, deleting links if no action by the user is taken within a reasonable time, or “block” lists could further enhance the system. FB-I has also introduced similar systems concerning “groups” or “removed friends”. There is no logical reason why this should not apply to “tags”.

➔ ***R25: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I ask the DPC to prevent such processing.***

7. Complaint 04 “Synchronizing”

A. Facts described in the original Complaint:

Facebook Ireland gives its users the possibility to “synchronize” mobile phones and other devices with the Facebook platform. This gives the user the possibility to find people they know on Facebook. For doing so the user must transfer all the personal data held in his device to the Facebook platform, Facebook Ireland then checks if they can find users by matching names, e-mails and other information.

After matching the users, Facebook Ireland does not delete the personal data it gathered, but saves it further for its very own purposes, such as promoting the platform and sending out invitation e-mails on behalf of the user. In this scenario it has to be noted, that not only the sender of the invitation is shown in these e-mails but all other users that Facebook believes the invited person might know. This includes people that have previously uploaded this e-mail by synchronizing. The actual data subjects do not have any possibility to prevent users from uploading this personal data. The data subjects also do not get informed about the processing by Facebook Ireland.

If a user does not want Facebook to know its work e-mail, but only a private e-mail, the user does not have any chance to prevent Facebook Ireland from gathering this information from one of the other users. The same is true for workplaces, telephone numbers and other information.

There is no consent by the data subject for this processing of personal data. The data subject might not even be a member of Facebook. When using Facebook Ireland’s “iPhone App” the user is not even asked if all data subjects gave their consent. The Software only asks if the data subjects are “comfortable” with the use of their personal data. There is also no hint that all the data will be used by Facebook Ireland for other purposes than just finding friends for the user (see attachment 03).

The idea that any user would actually ask all its hundreds of contacts if they are comfortable with the use of their personal data is more than absurd. It is also legally impossible that the user of the “iPhone App” consents to the use of someone else’s personal data. Only the data subjects can give their consent.

I think that a Facebook user can use the information he/she holds for the purpose of searching for friends on Facebook as a form of a purely private or household activity, as defined in section 3A(4)(c) DPA and Article 3 of the Directive 95/46/EC, as long as the information is not transferred to another party (such as Facebook Ireland). Any processing by Facebook Ireland which goes beyond its services as a host of the information cannot be legitimate without the specific consent of the actual data subject. Facebook Ireland is clearly mixing its role as host/processor with its role as a controller of the data and two different purposes of processing for its own benefits.

B. Additional Submission of Facts:

Other Forms of Importing Users' Data

Despite criticism of the ODPC in the first report, FB-I still allows users to import up to 5.000 (!) e-mail addresses to invite people to a new "page". There is no way that FB-I is getting valid consent to the processing of this information and the "audit" and the technical analysis only lead to a "geo block" of users in the EU/EEA. I am wondering how this is done e.g. when a European user uses a ".com" e-mail. In addition the report does not investigate about the further use of this data by FB-I. I also want to stress that Ireland is responsible for all users outside of the US and Canada. There is no reason whatsoever that the same steps were not also taken for users in other countries.

➔ ***F39: There was no adequate response concerning the option to "import" data on pages.***

Results from Data Gathering

In my data set the results of this practice became especially obvious. I am using my University email for facebook.com and removed all other email addresses. However FB-I is still using my main email ([REDACTED]) and another email that never existed ([REDACTED]) and links them to my profile. The second email seems to be a misunderstanding as I was working for "AFS", that hold the URL "afs.at" but this email never existed. Some person must have mistyped it and then "synced" it with facebook.com. All this can only be seen in the original data sets from 2011 and in the "download tool". There is no way to correct or remove this data and there is no way to object to FB-I keeping this information without my consent.

FB-I is using such information to "link" data of Facebook users with data from third parties, by hashing any linking email addresses used on different services. This is described above in connection with the use of data from "data brokers". Such addresses might however be incorrect or outdated and result in false analytics as the user is unaware of them and also unable to amend them.

➔ ***F40: There was no adequate possibility to remove or object to false and incurrent data gathered through synchronizing.***

C. Reaction by FB-I and the DPC:

The reports and the technical analysis did not uncover anything substantially new. The reports do not cover the legal claims of the initial complaint, but refer to the outcomes of the Canadian DPC's investigation and the investigation by the Hamburg DPC. I took a closer look at these investigations and came to the conclusion that the Canadian DPC was in essence again referring to the Hamburg DPC:

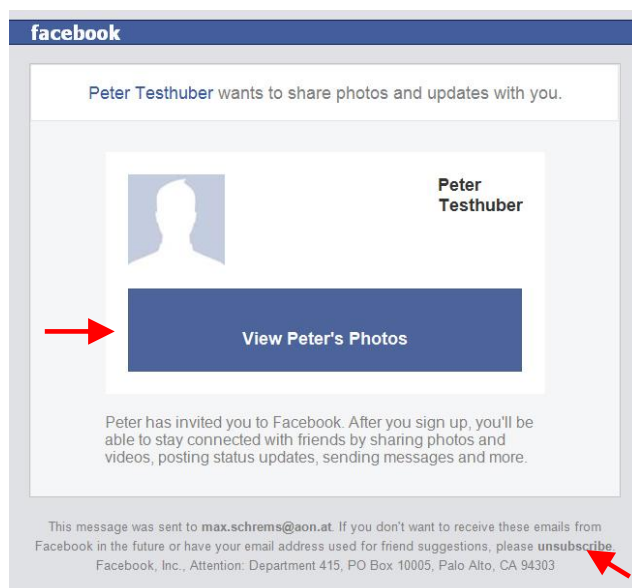
"When the complaints were filed, invitations provided little information about the process for providing friend suggestions. They also lacked a clear feature enabling recipients to opt-out of receiving further messages, or of having their email address used to generate friend suggestions. During the investigation, the company agreed to make a number of changes following discussions with our Office along with another international data protection office, which had related concerns. In particular, Facebook added a more user-friendly method to opt out of receiving friend suggestions or any further messages. As well, it removed friend suggestions from initial invitations and only sent these in subsequent reminders."

(Source: http://www.priv.gc.ca/media/nr-c/2012/bg_120404_e.asp)

The solution by the Hamburg DPC is only making sure that FB-I provides for an "opt-out" so that users do not get further emails and that FB-I only uses email addresses of its users for "matching friends" but not for other purposes. The initial invitation (see screenshot) is sent by other users of FB-I.

If the recipients do not click on the tiny "unsubscribe" button in the tiny grey text, FB-I is currently assuming that the users consent to getting further "invitations" by FB-I (others might call these "invitations" it simply "spam").

The text and the design of the invitation is controlled by FB-I. FB-I is using the subject "Check out my photos on Facebook" for this message – even though the test account did not hold a single photo(!). The recipient in this example is tricked into believing that the inviter wants to "share" pictures, in fact FB-I composed this message. While FB-I allowed to leave a small message previously, there is now *no* part of the "message" that is written by the user. It cannot be edited or even seen by the user.



In summary FB-I is telling the "sender" that he invites other people to Facebook while in reality the message says that the "sender" would like to "share photos and updates with you". In fact this is a blank lie.

The "sender" has nothing to do with the content of the message. He can only submit email addresses of other data subjects.

The "recipient" has never given any form of consent and has not even made any voluntary act.

In summary this is blank spam mail, with FB-I hiding behind a user that has no influence.

I therefore question FB-I's claim not to be sending the message themselves and not to be the controller. They are deciding about the content (even false and misleading content), the "sender" does not have any knowledge of the content and no possibility to edit it. FB-I is also running the infrastructure and the system that allows to "block" messages. Non-clicking of the "unsubscribe" button is also seen by FB-I as consent to have the data subjects' data be processed by FB-I – not the individual user. To be able to get that in line with the legal framework, FB-I has to be the "controller" or a "joint controller" of such invitations – this would at the same time make them a sender of spam mail.

- ➔ **F41: FB-I is controlling the content (even false and misleading) content of these invitations, runs the infrastructure and does not allow the "sender" to edit or even see the content.**
- ➔ **F42: It is not consequent to say that the individual user is responsible for the invitation and, but claiming that not clicking on the "unsubscribe" link is consenting to processing by FB-I.**

Agreement with the Hamburg DPC

The solution that was reached by the DPC in Hamburg was surely a step in the right direction. At the same time it is not in line with the duty to get an informed, specific and unambiguous consent.

If not clicking a tiny link, in a tiny gray text, in a message that users have never asked for constitutes informed and unambiguous consent, one can totally eliminate the idea of "consent" under the law. This form of consent is the total opposite everything that can be read in any law book or in WP187:

"The notion of "indication" is wide, but it seems to imply a need for action." (WP187, Page 12)

"For example, a data controller may have not have the certainty needed to assume consent in the following case: let us imagine a situation where upon sending a letter to customers informing them of an envisaged transfer of their data unless they object within 2 weeks, only 10% of the customers respond. In this example, it is contestable that the 90% that did not respond did indeed agree to the transfer. In such cases the data controller has no clear indication of the intention of data subjects." (WP187, Page 12)

"The fact that the individual did not undertake any positive action does not allow to be concluded that he gave his consent. Thus, it will not meet the requirement of unambiguous consent." (WP187, Page 24)

"Example: invalid consent for further uses of customer data An on-line book retailer sends an email to its loyalty program customers informing them that their data will be transferred to an advertising company, which plans to use it for marketing purposes. Users are given two weeks to respond to the email. They are informed that a lack of response will be deemed consent to the transfer. This type of mechanism, whereby consent is derived from a lack of reaction from individuals, does not deliver valid, unambiguous consent. It is not possible to ascertain without any doubt that individuals have agreed to the transfer from their lack of response." (WP187. Page 24)

"Consent based on an individual's inaction or silence would normally not constitute valid consent, especially in an on-line context." (WP187, Page 35)

Given this very clear picture, I have no doubts that there is no "unambiguous" consent when data subjects do not react to an e-mail. Otherwise there could be some claim in any spam email that would allow using all personal data of the recipient.

- ➔ **F43: Inaction following an email does never constitute informed and unambiguous consent.**

If a recipient does not care about the (non-existing) “pictures” or the user that invited him/her, the recipient might not even read the message. In such a situation the recipient has in no way given consent as he was not even able to see this text – let alone that also people that open such a message would hardly see this tiny gray text. If this is compared to the “sign up” process where the DPC has forced FB-I to change things one has to wonder about the rationale behind the reasoning deployed. When signing up there is at least some kind of action by a data subject. In this case the data subject might not even be aware that there is an email and has not taken any action whatsoever.

➔ ***F44: There is no reason to believe that recipients are reading or even seeing such a text. In many cases there is not even a voluntary “inaction” by data subjects. There is just nothing that could be dreamed of to be a valid consent.***

Legitimacy of the “agreement” with the Hamburg DPC

So why did the Hamburg DPC agree to such a system that is in clear breach of WP187, the German law and even the ECJs rulings (see e.g. C-92/09, 61-64)? The simple answer can be found in one of the last sentences of the press information on the webpage of the Hamburg DPC:

„Noch weitergehende Lösungen, etwa der (...) Verzicht auf das Importieren von Daten Dritter, waren in den Verhandlungen nicht zu erreichen. Sie dürften auch aus rechtlichen Gründen kaum durchsetzbar sein.“

In English: *„Broader solutions, for example a total abandonment of the import of third party data, were not possible to achieve in the negotiations. They would also for legal reasons probably not be enforceable.“*

In essence The Hamburg DPC found that it does not have jurisdiction over FB-I (see above “General Remark: Controller”). Therefore the Hamburg DPC has agreed to whatever it was able to get from FB-I through negotiations. This solution is therefore not the result of a formal procedure that was applying the law to FB-I but the result of a “deal” – where FB-I had any possibility to leave the table.

I am of the opinion that this step was reasonable given the conditions the Hamburg DPC was operating under, but this cannot be the bases for a decision by the Irish DPC, that clearly has jurisdiction over FB-I. Solutions have to be in line with the law and cannot be the result of a backroom “deal”.

➔ ***F45: The solution reached by the Hamburg DPC was a step in the right direction, but is not in line with the law or the common opinion within the EU (WP187).***

➔ ***F46: FB-I and the DPC were not able to deliver any counterarguments to my initial complaint.***

E. Amended Statement concerning Legal Consequences:

As the DPC has only referred to other DPCs and FB-I has not changed the way this function is working there is no reason why the initial claims would be incorrect. However as there are additional information I would like to amend my claims (in normal letters) – based on the original complaint (in *italic* letters):

1. *There is no specific and informed consent by the actual data subject. There is also no way to object or opt out of such data processing. This constitutes a breach of section 2A DPA and Article 7(a) of the Directive 95/46/EC. This makes any processing by Facebook Ireland illegitimate.*
2. *Facebook Ireland is using the personal data it gathers for the “matching process” as the primary purpose, but also for other secondary purposes such as advertising its own services. This breached the principle of purpose-based processing of personal data in section 2(1)(c) DPA and Article 6(b) of the Directive 95/46/EC.*
3. *The user of the “iPhone App” is left with the idea that she/he can consent to the use of another data subject’s personal data. The data subject has no chance to know, intervene or object to the processing of data that are submitted through third parties. This and the secret gathering of data through third parties additionally breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of the Directive 95/46/EC.*
4. There is no way to correct or remove false data. FB-I cannot ensure that the data is accurate, complete and kept up to date, which breaches section 2(1)(b) DPA and Article 6(1)(d) of the Directive 95/46/EC.
5. The data is kept for longer than necessary as old emails are not deleted or removed but stay in the system forever. This breaches section 2(1)(c)(iv) DPA and Article 6(1)(e) of the Directive 95/46/EC.

➔ **R26: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I ask the DPC to prevent such processing.**

➔ **R27: If the DPC is departing from the understanding of the law by the Article 29 Working Party I hereby ask the DPC to explain why it does.**

8. Complaint 05 “Deleted Postings”

A. Facts described in the Original Complaint:

About half a year to a year ago I decided that I wanted to delete as much of my personal data as possible on my facebook page. I used an automatic routine that automatically clicked on all “X”-buttons (labeled “remove post”) on my Facebook page. The following prompt clearly states that the content gets “deleted” (see attachment 03). After the routine was running for a while, all content was gone. From this point on I was continuously deleting all new content manually. In two or three cases old content kept coming back to my wall after I deleted it weeks earlier.

See attachment 04: A screenshot taken on the 1st of July 2011 (10 days before the file for the access request was created) where only two posts can be seen: one new (date: June 26th) and one old post that appeared again (date: April 23rd). This proves that all old posts were deleted, except the one post that came back. At the end of my Facebook page the system said clearly: “There are no more posts to show.”

After making an access request at Facebook Ireland, I got a 1.222 page PDF-File that listed personal information, including 11 random old “wall posts”, “shares” and “status updates” (see attachment 05). All of them have been deleted by me previously. It is unclear why only this random selection of posts still exists. Even today, these posts are not shown when I visit my facebook page, but apparently they still exist on Facebook Ireland’s databases.

These bits of personal data are rather old and should have been deleted by now even if the process of deleting may take some days or even weeks. The oldest piece of information is from the 21st of September 2008 (about 3 years old) and the most recent information is from the 10th of October 2011 (about half a year old). All of them were clearly deleted on the 1st of July as it can be seen on the screenshot in attachment 04. According to Facebook Ireland’s privacy policy data is only saved for 90 days as a backup copy, all posts in question are older than 90 days.

This information leaves me with two possible interpretations:

- a) Facebook Ireland is not deleting removed posts at all and sent me only some of my old posts by mistake. The fact that I deleted them must be saved in some way since the old posts do not show up on my wall anymore.*
- b) Facebook Ireland is not deleting some removed posts and is only making them “invisible”, while most other posts were actually removed.*

B. Reaction by FB-I and the DPC:

According to the December Report, FB-I has claimed that the deleted posts were only visible because they were still within the deletion period of 90 days. In fact FB-I says that I have deleted these postings approximately 12 days before the “access request” – which is in direct contrast of my submission certifying that I was deleting these postings “about half a year ago”.

There seems to be no facts that would support this claim by FB-I and this does also not make sense as the original screenshot clearly shows postings from April 23rd and June 26th – so before the 12 day period FB-I is claiming. There is also no clear explanation if FB-I refers to the production of the file (which would be July 11th 2011) or the filing of the access request (which would be June 2nd 2011).

I also miss a stringent explanation of why only some postings were available, while most postings were not in the file. Were the other undeleted postings not disclosed, or were other postings deleted?

➔ ***F47: The claims by FB-I are not supported by any form of evidence. They are in clear contrast to the facts and submissions I have made and are not stringent in any way.***

➔ ***R28: Therefore, I am asking the DPC to disclose the exact reaction by FB-I to in relation to this complaint, as well as possible evidence that was delivered in relation to this complaint. I also ask the DPC to let FB-I explain how they were able to come up with the exact number of “approximately 12 days” and how they calculated this exact number of days.***

Either way the claim by FB-I seems to be false. I have repeatedly used a Firefox Plug-In, called “iMacros”, which has automatically deleted all postings on my wall, as well as other Facebook data like my messages. A short video that shows how this works can be found [on YouTube](#). I have run the plug-in for the first time during the year 2010 or even earlier and the last time during the first half a year of 2011. I can recall this because this was before and during my studies in the US. The postings that were found in the data set were dating back to 2008 and 2009. This means that they must have been deleted when I have used the automatic script for the very first time in 2010. This would have been years before the 90 days and would surely include postings from 2008 and 2009. The claim by FB-I seems to be false and misleading. There is no evidence or other information that would constitute a reason to belief that FB-I is correct about the fact that it was only deleted 12 days prior to the access request or the production of the PDF file FB-I was sending to me.

➔ ***F47: While I cannot recall the exact times, I hereby certify that I have deleted all of my Facebook “wall” repeatedly and long times before the 90 day period that FB-I relies on.***

C. Legal Consequences described in the Original Complaints:

I think that this processing by Facebook Ireland is illegal under the following provisions:

- 1. There is no transparent notice that these bits of data are still held. In contrast to that the user is told that the content is “removed”, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
- 2. There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.*
- 3. There is no longer a legitimate purpose for holding on to these bits of data. There is no other purpose specified by Facebook Ireland. The data would have to be deleted according to section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
- 4. The further processing of these bits of data is no longer relevant for the purpose of the processing and seems to be also excessive, which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
- 5. The processing of the data seems to be longer than necessary to fulfill the purpose and therefore seems to be no longer necessary. This would constitute a breach of section 2(1)(c)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*
- 6. It seems that there has never been an informed consent by the user to the use of these bits of data since the user just agreed to the processing with having the option to “remove” this content later. If Facebook Ireland does not remove this content, the consent is neither informed nor unambiguous and therefore void under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*

In addition I want to add the following claim:

- 7. It seems that there has never been an informed consent by the user to the use of these bits of data since the user just agreed to the processing with having the option to “remove” this content later. If Facebook Ireland does not remove this content, the consent is neither informed nor unambiguous and therefore void under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*

➔ R29: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I ask the DPC to prevent such processing.

9. Complaint 06 “Posting on other Users’ Pages”

A. Facts described in the Original Complaint:

Like many other platforms facebook.com allows users to comment on other users’ objects (e.g. posts, photos, videos). On most platforms the user can comment anonymously, but therefore knows that his/her comment will be visible to anyone accessing the page.

Facebook Ireland is doing this differently: All postings are shown with the user’s real names and at the same time it is possible to limit the visibility to other people. This makes the user believe that he/she is sharing the information only with his/her friends. In fact the user has no idea who he is sharing the information with:

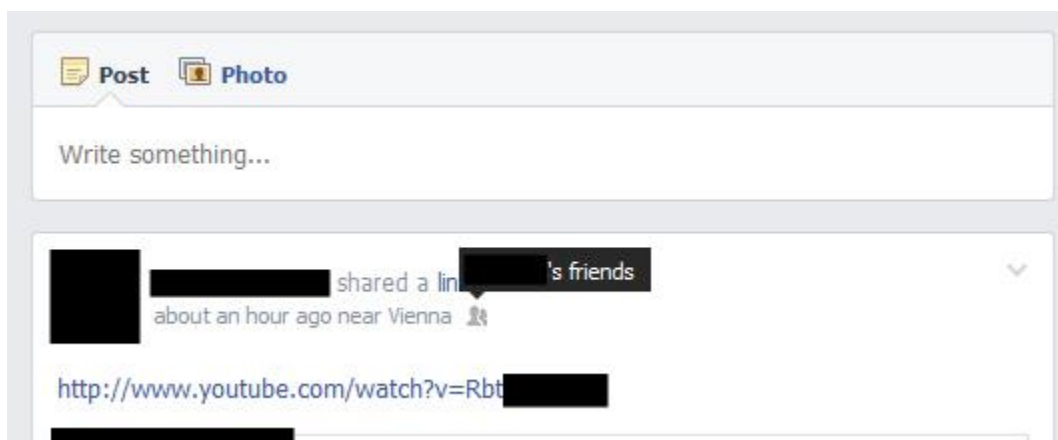
“When you post information on another user’s profile or comment on another user’s post, that information will be subject to the other user’s privacy settings.” (Facebook Ireland’s privacy policy)

There is no symbol or information that would show the user the settings that would control the posting (see attachment 03). The user is blindly posting something, not knowing if it will only show up at the other users “friends” (130 people), “friends of friends” (16.900 people) or “everyone” on the internet, including search engines.

B. Reaction by FB-I and the DPC:

Introduction of a new System by FB-I

I am happy to see that FB-I has made great progress in respect to this complaint by implementing a system where data subjects can see the audience of another users’ page they comment on. The report points out the functions and I have nothing further to add at this point.



Screenshot: FB-I now displays the audience of a friends’ posting.

➔ **F48: FB-I has changed towards a model that I suggested in the initial complain, which shows that the initial complaint was fully justified.**

Remaining Problem: Change of Audience / Simple Solutions

FB-I's new solution also has a drawback that I have pointed out in previous exchange with the ODPC: Data subjects can only consent in an "informed" and "specific" way. The main information that data subjects will consider before posting is the audience of a posting. FB-I displays the audience set by the owner of the page, but it also allows users to change to more public settings after another person has posted something or reacted to the posting (e.g. from "friends only" to "public").

It is a cornerstone of facebook.com to make people believe that they exchange among their friends and that it is not public if one user posts on another users' page. Only through this system FB-I gets users to open up under their real name in a way they would never do on a public blog or discussion forum. Any consent to share such information is always based on the data subjects' understanding of the audience that can see such information. This is undermined if users can switch the postings from "friends" to "public", making any comment viewable and searchable for anyone in the world.

In this respect the ODPC has taken the following position in the second report from September 2012:

"This Office has considered this issue in detail (...) and is inclined to the view that if a Facebook user chooses to post on another Facebook user's page that they do not do so with an expectation that the post will be either private or restricted to an audience that they are comfortable with." (Second Report, Page 49)

The ODPC further noted:

"If a user has a concern about the audience for a post they make or that the audience might be subsequently expanded from say 'friends only' to 'public' then there is a simple solution available to them and that is not to post on other user's pages." (Second Report, Page 49)

The second argument can be deployed in a privacy discussion in a local pub, but has nothing to do with the law. If this argument is consequently deployed any controller in the world could just make any information it has public, despite consent by data subjects that did not include the publication of such data. In the end this would be the end of any meaning of the "consent" model.

In addition it was the core idea (supported by the ODPC) that other users should get information about the audience in order to make informed decisions. It is not stringent to also allow a later change in the audience after such an "informed decision" has taken place.

The only (legal) "simple solution" would be that FB-I is adding a control loop whenever a user is changing setting from a restrictive to a more liberal setting and prohibits such changes whenever other users have commented, liked or otherwise added information to such a posting.

- ➔ **F49: FB-I allows to change the audience of a posting (the core criteria for a valid "consent") after the consent was given. The ODPC seems to have no problem with this.**
- ➔ **R30: I urgently ask the DPC to name the provision of the Irish Data Protection Act from which it has derived this "simple solution", since I was unable to find it.**

C. Legal Consequences described in the Original Complaint:

1. *There is no transparent notice that indicates the group of people that will be able to see the post. This breaches the principle of fairness in section 2(1)(a) and section 2D DPA and Article 6 (1)(a) of Directive 95/46/EC.*
2. *It seems that there has never been an informed consent by the user to the use of these posts since the user has no idea of the extent of people he is sharing information with. Without an informed consent any processing is illegitimate under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*

D. Additional Statement on the Legal Consequences:

In addition there is no proper information about this possible change of audience by FB-I or the users and the use of such data that was initially private and is then published would also be a form of “further processing” that would in no way be compliant with the original purpose. Therefore I would like to add the following two claims:

3. There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.
4. The “further processing” of this data does not seem to be “compatible” with the initial purpose in most cases which constitutes a breach of 2(1)(c)(ii) DPA and Article 6(1)(b) of Directive 95/46/EC.

➔ ***R31: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I ask the DPC to prevent such processing.***

During the past two year I had to see that neither the FB-I nor the ODPC have elaborated about the question who the controller of a page/“timeline” is. I also had to see that original complaint is not making this fully clear. If the DPC is following the idea that the user of a timeline is the controller then this problem is not a direct breach of the law by FB-I.

However if FB-I is then further using this data as being “public” then FB-I would use data that was obtained against the law – which consequently means that FB-I would also not be allowed to use such data as “public” data, but only in line with the original settings.

➔ ***R32: If the DPC is sharing this view I hereby – involuntarily – ask the DPC to render the legal claims to only cover the further use by FB-I that is incompliant with the original settings.***

10. Complaint 07 “Messages”

A. Facts described in the Original Complaint:

Facebook Ireland offers all users of facebook.com a messaging and chat service. Very recently Facebook Ireland merged its messaging and chat function into one messaging function. Users can send messages to each other, just like an e-mail but they are also displayed in a chat window with very little delay if both users are online. Unlike e-mails, all messages are held on Facebook Ireland’s systems and the actual messages are never delivered to the users’ systems.

Facebook Ireland’s users have about the same options as users of usual “webmail” services (e.g. making messages as unread, replying and deleting the messages). After Facebook Ireland recently changed the system, all messages (including chat messages) can also be “archived” (see screenshots in attachment 03). When the user clicks on “delete messages” facebook.com is showing a prompt which tells the user that the deletion of the message cannot be undone (see attachment 04). In fact messages are not deleted. 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 (see attachment 05).

If the user digs through the 12 page privacy policy, he/she will find the following provision:

“Certain types of communications that you send to other users cannot be removed, such as messages.”

Note: This provision can be found under the section “3. Sharing Information on Facebook”, subsection “Other”. This is fact is not mentioned under the section where users would actually look for such information “7. How you can change or remove information”.

Messages are generally treated as very sensitive information (privacy of correspondence). This must be even more the case if the messages are stored on servers within the US (see Facebook Ireland’s terms, section 16.1). The United States does not have a protection of correspondence similar to the European level under Art. 8 ECHR, this is especially true for information of foreign citizens.

It seems disproportional that information that was published on the user’s wall can be deleted, while more personal and private messages will be saved on Facebook Ireland’s systems forever. I could also not find any other “chat” service that would save all sent messages with the users’ real names for an indefinite time.

Facebook Ireland announced that it is now planning that all users get their own ‘facebook.com’ e-mail address. Facebook Ireland wants that all users use facebook.com as their main provider for electronic communication, which would mean that all electronic communication would be stored by Facebook Ireland for an indefinite time.

At the time when Facebook Ireland becomes an e-mail provider these rules would also apply to messages that were sent from data subjects that are not even member of facebook.com. Third party senders of an e-mail would fall under this regime without any form of information, consent or legitimacy.

If this scenario is compared to the European Data Retention Directive (2006/24/EC), it seems very clear that it is disproportionate: The information is a) never deleted, b) consisting of not only traffic, but also content data, c) hosted with very limited data security, d) analyzed by the processor and e) held on a territory where the information is not protected from law enforcement agencies and secret services in a way that is common within the European Union.

B. Reaction by FB-I and the DPC:

Retrieval of “Deleted” Messages through others’ Inboxes

The reports and technical analysis are helpful to get a broader insight of how FB-I processes deleted messages. At the same time there are certain inconsistencies of the technical report with the facts I found. For example the report suggests that once a user has deleted his “outbox”, it is not possible to find corresponding messages in the “inboxes” of the hundreds of recipients:

“Another alternative would be to scan all other cells in Titan [FB-I’s storage system] 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.” (Technical Report in the “Review”, page 51)

This finding is absolutely false if it is compared to the evidence I have submitted. FB-I was able to deliver all messages that were deleted when supplying me with the response to the initial access request (there were about 300 pages of “deleted” messages). FB-I has claimed that these messages were not deleted because it was in the “inbox” of other users, as I have anticipated in the initial complaint. This fact demonstrate that 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.

➔ ***F50: FB-I is able to retrieve all deleted messages from the system, no matter where they are stored. The facts of the “technical analysis” are simply false if compared with factual evidence.***

FB-I has further argued that messages are fully deleted when all data subjects that have been part of the conversation have deleted the message. I cannot see any facts or material arguments that would support this claim in the reports or the technical analysis.

➔ ***F51: There is no evidence that messages are deleted when all users have deleted their individual copy of the message.***

Analytics of Content Data

FB-I claimed that it is not processing the content of a message. There has not been any fact based evidence supporting this claim. There are facts that indicate that FB-I uses non-content data of personal messages and recently FB-I has said that it also scans the content for different filters and an alert system aiming at child predators. The technical analysis of the report only says that

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

There is also no provision in FB-I's privacy policy that would hinder FB-I from processing the content of messages for any purpose (like e.g. advertisement or friend suggestions). The difference between content and other message data is not reflected in the policy. To the contrary "messages" are listed in the general section about "information we receive about you". All this data is only governed by one provision in the policy which allows for any practically operation:

"We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use."

As outlined in the section on "shadow profiles" there are a number of cases where there was a significant relationship between the suggestions (e.g. my hometown) and the number of times a town was named in old or even deleted messages. Without this fact there would be no logical basis to e.g. suggest "New Orleans" to be my hometown.

➔ ***F52: There is no fact based evidence of the extent of processing of the content of messages. FB-I's own privacy policy does not limit the use of content of messages for any purpose.***

C. Additional Statement on the Legal Consequences:

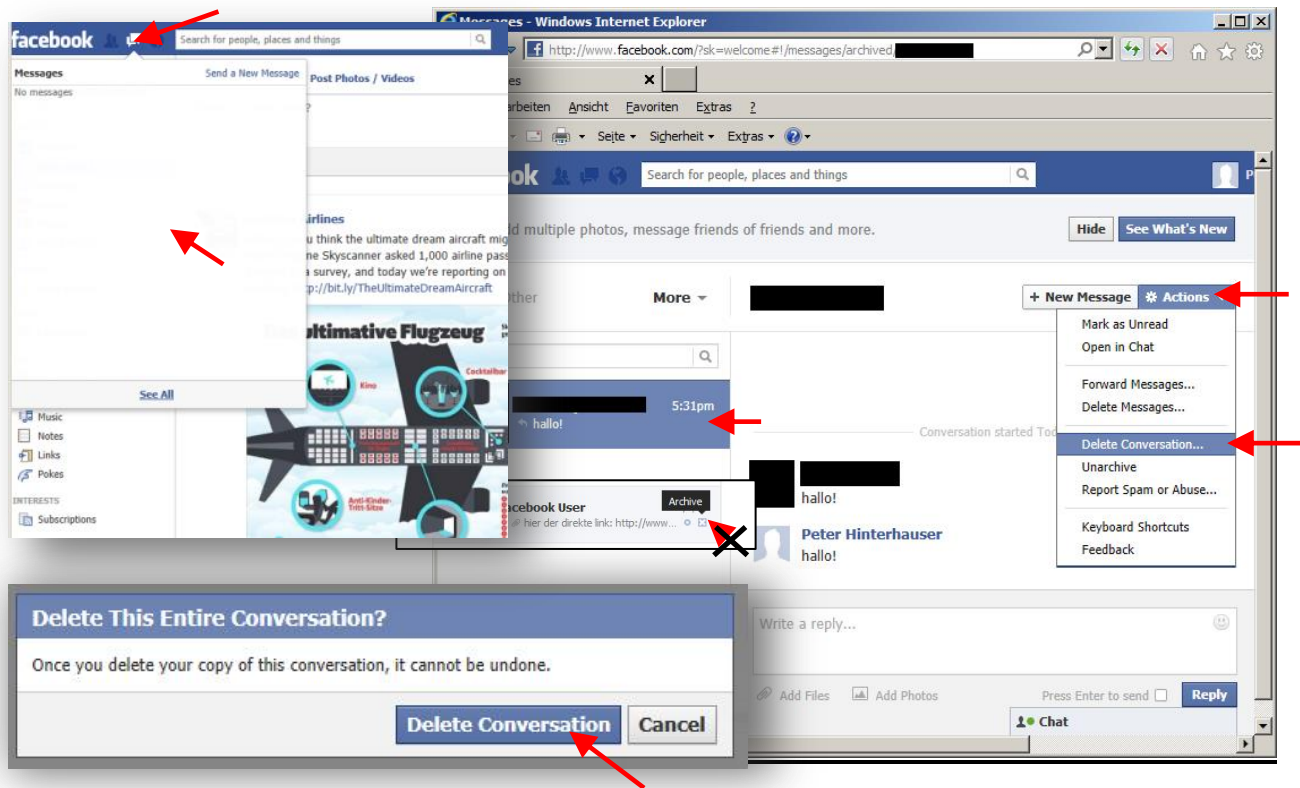
Material Problem

Independent from these factual problems the "audit" have not dealt with the material claim in the initial complaint, which is in essence that the system itself might work reasonable in respect to each detail of the operation, but that the overall result of the processing is excessive given the purpose. I am aware that this is a complicated issue, but this is the core of the complaint after all so I urge the DPC to review this issue thoroughly and give it the necessary time any evaluation.

a) Deletion Process

FB-I generates endless amounts of personal, private chat messages that *can factually* not be deleted. All users that have communicated via facebook.com have to "delete" every single conversation, which takes 6 clicks from the start page. If a user would want to delete all his/her copies it would take hours.

There is no way for "mass deletion" and FB-I does not automatically "delete" old chats, like every other chat system I am aware of does and how FB-I has itself originally done. The merger between "chats" and "messages" has further lead to a system where every little exchange of information is treated like highly relevant personal email. This does not reflect the users' reality and is an exceptional approach that cannot be seen anywhere else in the world.



Screenshots: Deletion of a copy of a chat conversation through the user.

- **F53: It is practically impossible for users to delete all their messages with reasonable efforts. There is no automatic deletion after a certain time and no option for “mass deletion”.**



Screenshot: FB-I is still using the word “delete” – despite the fact that the message is kept.

- **F54: FB-I is still saying that messages are “deleted”, despite the fact that they are kept on the servers.**

b) Comparison to E-Mail and Chat Programs

If the messaging system of FB-I is compared to emails I want to stress, that emails do not work in a similar fashion, since the “inbox” and “outbox” of the different users are spread out all over the personal computers of every individual user or maybe situated at their provider (webmail).

If a user deletes his set of e-mails it is factually impossible to find the corresponding e-mails in the outbox or inbox of the other recipients because no one can reconstruct the communication and is therefore unable to know about the other recipients.

This is totally different on facebook.com as my original data set has demonstrated. In addition normal software (like “Outlook”) on a users’ computer makes the user archive or delete old messages and offers many options to get rid of old emails (e.g. mass deletion of all messages with a couple of clicks).

In comparison to systems that are closer to what a user expects from a “chat” like the one offered on facebook.com it is more than obvious that all these services delete chats within a very short period of a couple of hours or days. There is never an endless storage of all private messages in a central location.

➔ ***F55: FB-I’s chat system is designed inherently different than other systems that offer similar functionality, since these systems do not allow to centrally retrieve all old and deleted messages.***

c) Government Access

In addition 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. In the US (where the servers are situated) there is not even a constitutional right to privacy when messages are stored on a central system. This legal way to access such data has to be taken into consideration when assessing the risk of privacy violations.

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. This is an impact on the privacy of the data subjects that can in no way be “not excessive”. While one can argue how much this has to be accepted as “Facebook Inc” is subject to US laws there is surely no why the DPC could not limit the existence of such highly sensitive communication data at FB-I. If such data is not harvested without any practical use and need there is also nothing a US authority could later retrieve – without any probable cause of judicial oversight in the individual case.

➔ ***F56: FB-I’s centralized system is a heaven for authorities that want to access endless amounts of information in one place and without the knowledge of the data subjects.***

d) Surveillance by Design

In summary we are looking at a system that might not be intentionally aimed at getting users into this position, but does in fact generate endless amounts of junk data (= old chats) that can practically not be deleted by the individual users, since it can always be retrieved through the counterparts of the copies. The system that FB-I has generated does not follow the idea of “privacy by design” but could rather be described as “surveillance by design”.

The law does not only cover intentional threats to the right to data protection of the individual, but is mainly covering systematic problems that bear a tremendous factual risk of a breach of the right to privacy of data subjects. This is the preventative character of the law, which must clearly be triggered by this system and the risks that I mentioned above.

Facebook.com was initially designed as a student project, but since it has become a standard form of communication and for some the main form of communication, a design that is in fact making every single message centrally retrievable, independent from the deletion by the user cannot be in line with the principles set out in Section 2 DPA and Article 6 of Directive 95/46/EC.

➔ ***F57: FB-I’s centralized system might not be intentionally aimed at keeping everything about everyone, but is factually doing just that. The law is covering any form of processing – not only processing that is intentionally infringing the privacy of data subjects.***

e) Comparison with “Data Retention Directive”

As the ECJ has held that Directive 95/46/EC has to be interpreted in line with Article 8 ECHR (C-465/00). This means that also private companies have to follow the limitations under the ECHR when processing personal data. This is the fact for FB-I as much as for any other company operating in Europe.

The “Data Retention Directive” (2006/24/EC) is generally viewed as the most extreme measure one can possibly get in line with Article 8 ECHR. The question if this law is in line with the fundamental rights of citizens is currently before the ECJ through court referrals from Ireland and Austria. However this system only covers meta data, is only limited to a retention period 6 months and there are strict rules about the use of such data. However a number of courts in the EU have ruled that it is unconstitutional.

If e.g. “Eircom” would tomorrow start to keep a record of every email, text message or phone call in a centrally stored location and would only allow customers to manually delete this conversation on an “per item” basis (rendering it factually impossible to do so) and additionally requiring *all* participants of a communication to delete this data in order to fully remove it, no one in the world would have a hard time to see that this is in no way compliant with Article 8 ECHR. This would be even more so if there is more than just probable cause to believe that “Eircom” would grant access to all this data by the NSA.

For many people of my generation FB-I has replaced more traditional forms of communication. There is no obvious reasons why an allocation of data to the extent that would be unbelievable in area of “traditional” communication providers should be treated radically different in respect to new communications providers.

In addition I want to say that FB-I has a factual monopoly for online chats. It has absolutely replaces any other IM service for most users. But even if people are trying to avoid exchanging messages on facebook.com (as I usually do) there is no way around other users contacting a person.

- ➔ **F58: If FB-I's system is compared with any other communications provider it becomes obvious how this system can in no way be compliant with Art 8 ECHR.**
- ➔ **F59: FB-I also has a factual monopoly on instant messaging (IM) which means that most data subjects have no possibility to avoid this system.**

D. Legal Consequences described in the Original Complaint:

I think this processing by Facebook Ireland is illegitimate under the Irish Data Protection Act and the Directive 95/46/EC for the following reasons:

1. *It seems that there has never been an informed consent by the user to the use of this information since the user just agreed to the processing with having the option to "delete" messages later. If Facebook Ireland does not delete any messages, the consent seems to be neither informed nor unambiguous and therefore void under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*
 2. *There is no transparent notice that these bits of data are still held after the user has clicked the "delete" button. In contrast to that, the user is told that the messages are "deleted", which breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
 3. *There is only (well hidden) information about the non-deletion of data in Facebook Ireland's privacy policy. Accurate information is needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.*
 4. *After both users have deleted the message, there is no longer a legitimate purpose for holding on to this data. The data would have to be deleted according to section 2(1)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
 5. *The further processing of this personal data is no longer relevant for the purpose of the processing, which constitutes a breach of 2(1)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*
 6. *The indefinite storage of personal messages (especially chat messages) seems to be extremely excessive, which constitutes another breach of 2(1)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*
 7. *The processing of the data seems to be longer than necessary to fulfill the purpose and therefore seems to be no longer necessary. This would constitute a breach of section 2(1)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*
- ➔ **R33: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I ask the DPC to prevent such processing.**

11. Complaint 08 “Privacy Policy and Consent”

A. Facts described in the Original Complaint:

Facebook Ireland is basing all processing of data on facebook.com on the consent to its privacy policy. Facebook Ireland holds excessive amounts of personal data, many of which is sensitive information (see personal data in attachment 03). Facebook Ireland is processing the data for multiple purposes. The data subjects are average (or even inexperienced) consumers in 192 countries worldwide.

Following the principle of proportionality this would mean that Facebook Ireland would have to publish very clear, easy to understand and at the same time detailed information about its processing.

1. Privacy Policy

As a first step I would like to analyze the privacy information that is given by Facebook Ireland and that the user is asked to consent to (see privacy policy in attachment 04).

a. Access

A link named “privacy” can be found on the very bottom of all pages of facebook.com. It is often times hard to scroll all the way to the bottom, since the start page expands about three times whenever the user reaches the end of the page.

If the user clickes on the link he/she does not see the privacy policy but a “privacy guide” that gives very limited information if compared to the actual privacy policy. The most disturbing information (e.g. that many things can never be deleted again) cannot be found here (see attachment 05).

On this “privacy guide” page, there is a link in the fifth line “read our privacy policy” that brings the user to the actual privacy policy. During the sign-up-process the user can see a little link that directly links to the privacy policy on one of the second page of the sign-up process.

b. Role of Facebook Ireland and the user

One of the most basic questions for any form of processing of personal data is the role of the different entities. Facebook Ireland does not specify in any way who actually is the controller, processor and data subject when data is processed on facebook.com. Many problems arise out of the uncertainty who is having ultimate responsibility for a breach of privacy laws on facebook.com.

Generally a data subject cannot specifically consent to the processing of his/her personal data, if he/she does not even know who is or will be the actual controller.

c. Extent of the privacy information

If printed in normal size letters, the privacy policy is 12 pages long (see attachment 04). Other privacy relevant information can be found in Facebook Ireland’s terms (attachment 01) and the “privacy guide” (attachment 05). This means the data subject has to deal with three primary documents. The privacy policy is not very well structured and many provisions cannot be found easily.

In addition, the policy links to countless other pages that hold even more relevant (and irrelevant) information (see chart in attachment 06). If the user follows these links, he/she will end up finding more than 200 pages of additional information that governs or further explains Facebook Ireland’s processing of personal data (see a selection in attachment 07).

d. Contradictions

Facebook Ireland's privacy policy is contradictory in many details, to list all contradictions would be too much for this complaint, but please take a look at the information issues in other complaints.

As an example I picked the different provisions in this system of policies concerning the deletion/removal of data (see attachment 08). Note that these provisions and information are 6 (!) pages long.

For example, Facebook Ireland states in one section:

"If you are uncomfortable with sharing your profile picture, you should delete it."

At the same time it states at some other place in its policy:

*"Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users."
(Note: profile pictures are always shared with everyone).*

Facebook also states in its terms:

"For content (...) like photos (...) you specifically give us the following permission (...): you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."

Summary: If a user is uncomfortable with sharing his/her picture, he/she can delete it, but it may be further used by others and Facebook Ireland. The first provision turns out to be contradictory to the other provisions, because deleting the picture will not necessarily help the user's privacy concerns.

At the same time Facebook Ireland states that it is following these provisions of "TRUSTe": "Participant must implement reasonable mechanisms to allow the Client or Individual to request deletion of PII or that collected PII no longer be used" and "Provide a reasonable and appropriate mechanism to allow the Individual request deletion or deactivation of a profile."

Apparently Facebook Ireland is not following this set of rules, as we can deduct from the contradictory statements above.

e. Vague provisions

Similarly to the issue of rather contradictory provisions, many provisions are also very vague. As an example I picked the provision of the privacy policy (attachment 04) explaining how Facebook Ireland is using all personal data. In fact this whole section consists of only one binding provision that governs all personal data:

"We use the information we collect to try to provide a safe, efficient, and customized experience."

It is very hard to think of a more vague provision than "providing a safe, efficient, and customized experience", every company (e. g. car dealers, gyms, shops, airlines) tries to do so. This meaningless

sentence is actually the only one controlling Facebook Ireland's use of the data subjects' personal information.

This general provision is accompanied by some examples how this might/can/could be done:

"Here are some of the details on how we do that (...)"

The following examples are by far not covering all the forms of processing by Facebook Ireland and even these examples are very vague.

2. Consent to the Privacy Policy

In this second step I want to analyze the user's consent to Facebook Ireland's processing of personal data as necessary under section 2A(1)(a) DPA and Article 7(a) Directive 95/46/EC.

a. Unambiguous Consent

The consent to the processing of data has to be made unambiguously. This means that the data subject needs to actively consent and the consent cannot be implied. This can be achieved by making the data subject tick a box to consent to the privacy policy (see e.g. Denis Kelleher, *Privacy and Data Protection Law in Ireland*, page 210).

Facebook Ireland is using one of the most nebulous ways of gathering the data subjects consent during its sign-up process:

- The consent to the privacy policy is included in a page that is titled "security check" (see attachment 08b). The user has to identify letters in a picture and write them in a text box and then click on a "sign-up" button.
- This security measure distracts the user from the little text that claims that the user is now consenting to the privacy policy and terms.
- The text claiming that the user is now consenting is underneath all the three elements the user has to interact with (picture, text box and button).
- The page directs the user to a center of attention while the actual text that informs the user about the consent to the privacy policy is outside of this center of attention (see attachment 09)
- There is no check box (or other form of unambiguous consent) that has to be ticked.
- The text that informs the user about the consent is the text with the smallest print on the whole page. All other elements (especially the one that the user has to interact with) are in much bigger print (see attachment 10)
- Colors and contrast are used in a way that further distracts the user from the text that informs him/her about his/her consent to the privacy policy.

While all three interactive elements are black/white or in green color, the text that claims the consent of the data subject is in grey tones. The contrast of this text is much lower due to a lighter grey of the text and a darker background than in other areas of the "security check" page (see attachment 11).

- Facebook Ireland is not using anything like a check-box that has to be ticked.
- Facebook Ireland has recently changed the page, which lead to an even bigger button, while the text that claims that the data subject is consenting has moved even further down the page (see attachment 12).

b. Freely given Consent

Facebook Ireland has a factual monopoly in most European and international markets. This means that an average user has no other option than joining facebook.com if they want to get engaged in social networks. Other pages have specific audiences (e.g. XING or LinkedIn) or have only a regional audience (e.g. the German "VZ"-networks).

Since there is not really any other option, the free will of the data subject (consumer) is so far limited to one realistic option, which is facebook.com. Even if the data subject might have seen the little text claiming that he/she has consented and has read and understood all of the privacy policy (see letters c – e below), it is very likely that these users will click on the "sign up" button without really expressing his/her free will.

The problem of factual monopolies generally leads to a very tough test on contracts, terms and conditions that these monopolies are using. I think this higher standard has to be applied to Facebook Ireland in particular because of the very limited competition.

c. Specific Consent

After analyzing Facebook Ireland's practices and policies for an extent time, I am convinced that there is no specific consent.

This starts with the specification of who is actually the controller / processor and data subject and goes on to the kinds of data that are processed, the specific purpose and the possibilities to delete information. The privacy policy is very vague and does not specifically clarify Facebook Ireland's handling of the gathered data (see above, "1. Policy"):

"We use the information we collect to try to provide a safe, efficient, and customized experience."

If we look just at the example given at section 1.e. of this complaint, it is easy to see that the user is consenting to anything but a specific form of processing of his/her data. What could be more of a general (and therefore illegitimate) statement than "We use the information we collect to try to provide a safe, efficient, and customized experience."?

Facebook Ireland even claims that the data subject is 'consenting' to the processing that anyone is uploading to facebook.com in the future and any information that Facebook Ireland is gathering from unspecified sources. The data subject also 'consents' to the use by any unspecified third party that runs applications that one of the data subject's friends happen to use.

This means that the user is e.g. 'consenting' to the processing and publication of an embarrassing picture that someone else will take and upload (without his consent) in some future day. In addition, a third party operator of an application may process this picture further for whatever purpose, as long as one of the data subject's friends consents to that. All these "consents" are prime examples of a non-specific consent.

At this point Facebook Ireland frequently argues that the users have the option to remove such content. This argument is irrelevant for two reasons:

1) The DPA and the Directive 95/46/EC do not allow replacing the specific consent with an "option to remove". The burden of the controller to get the consent cannot be replaced by the burden for the data subject to constantly check for data and remove it manually.

2) Most of this information (e.g. a "tag" in a picture) is only deactivated when a user removes it, while Facebook Ireland is still processing it in the background (see other complaints).

d. Informed Consent

If Facebook Ireland's practice is compared to the minimal standard set down in section 2D(2) DPA, it is clear that the information given by Facebook Ireland is not sufficient:

Facebook Ireland is not even properly disclosing its identity (section 2D(2)(a) DPA). In its privacy policy the first sentence leads the data subject to its parent company in the US: "contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304" (see attachment 04). The only hint to Facebook Ireland that can be found, is hidden in its terms under section "18. Other", subsection 1 where the user may find a company named "Facebook Ireland Limited", without an address, telephone number, e-mail or any other form of further information (see attachment 01).

The purpose for which the individual information is processed is not properly disclosed (section 2D(2)(c) DPA) as explained above (see 1.d., 1.e. and 2.c. above). Even after questioning Facebook Ireland via email they were unable to name me the specific purpose of processing my personal data (see attachment 13).

There are very invasive forms of processing (e.g. face recognition, publishing on the internet without limitations, very limited possibilities of deleting data) that are rather hidden than highlighted. This is contradictory to the "red-hand" rule. (see e.g. Denis Kelleher, Privacy and Data Protection Law in Ireland, page 218). Generally it is very likely that the data subject does not expect such forms of processing, so that he/she must be especially informed about this.

The rest of the given information is vague, unclear, poorly arranged and contradictory (see above).

e. Consent obtained by deception or misinterpretation

There are many cases where Facebook Ireland gives wrong, misleading or deceptive information. Many of them can be found in my other complaints, here are some examples:

- *Facebook Ireland constantly stresses that users are only sharing with their friends and that the user has control over all data he/she is sharing.
In fact, even the most private information is always visible to and used by Facebook Ireland for its purposes. The data subject can only limit what others can see, but he/she can never limit Facebook Ireland's processing. Over the time Facebook also changed the default privacy settings. Today most private information is now shared with anyone on the internet and indexed by search engines, if the user does not know how to change the settings.*
- *The users are told that their content is "removed" while in fact this is often times not possible (e.g. pokes, wall posts, messages).*
- *Functions like "deleting" the account are hidden on some help page, but can not be found in the normal menu.*
- *The "synchronizing" functions are not telling the user that Facebook Ireland is going to use the gathered information for more than only an initial matching process.*
- *Data subjects have the option to delete messages on facebook.com, while in fact they will be kept on Facebook Ireland's systems.*
- *Even in the privacy policy the user is told that he/she can remove tags or profile pictures while in fact they are only deactivated.*

B. Reaction by FB-I and the DPC

Content of the “Old Policy”

Since I have filed my initial complaints in August 2011, FB-I has changed its privacy policy three times. I want to point at WP187 specifying the level and form of information, which especially very complex systems have to be accompanied with (see WP187 page 21).

The “audit” seemed to be no helpful resource in this respect e.g. on pages 35 to 38 of the first “audit” report the ODPC in only listing my claims and a subsequent reaction by FB-I that does not deliver any meaningful reaction. FB-I is generally only expressing that it “*does not share the complaints view*”. From the current level of information I cannot see that any material counterarguments were brought forward concerning my initial complaints.

Because of the limited information I got through the report, I cannot really respond to the counterarguments to my original complaints. But I understand the ODPC’s findings in the report of December 2011 to be very much supporting my view and see nothing that would be contrary to the claims in my initial complaint.

→ ***F60: I face total absence of material counterarguments by FB-I concerning the content of the old policy. I can therefore not see that FB-I has brought anything forward that would question my original claims. To the contrary the changed FB-I has undertaken (see below) support my views.***

Content of the “New Policy” and new “Inline Control”

I very much welcomed that FB-I now has a single document and stopped linking to hundreds of other pages in its policy. At the same time the new policy is still of extreme length, extremely vague and impossible to understand for a normal user. After working with this policy for almost two years, it is still not possible for me or any other the member of “europe-v-facebook.org” to exactly say what FB-I does or does not do with users’ data, based on this policy.

The first “audit” report by the ODPC of December 2011 has to my view outlined many important things concerning the current policy. I especially want to point at the findings on pages 39 to 41. When looking at the changes by FB-I and the “review” from September 2012, I had to find that not much of these findings were in the end implemented. The change in the policy is in the end just a minor “face lift” that in fact mainly deprives users of rights and allows FB-I to process data in an even broader way. The new policy has not led to any limitation of FB-I’s use of data.

Length of the “New Policy”

I believe that there are ways to limit the length of the policy to a couple of pages, if FB-I puts some effort into it. Currently it seems that FB-I rather puts a lot of effort in a lengthy policy in order to deter users from reading and understanding it. In a legendary comparison the “New York Times” has shown that FB-I’s policy has become longer than the US Constitution. By now it has more than twice the length, amounting to 9.325 words. At a fast reading rate of 200 words per minute (which is unlikely to be the factual rate of consumers reading a complicated legal text) it would take a data subject more than 45 minutes (!) to read the whole privacy policy.

➔ **F61: FB-I’s policy takes more than 45 minutes (!) to read for an experienced reader or legal text.**

“Inline Control”

I welcome the approach of “inline” consent for every function. I have myself suggested to get specific consent every time a user uses a new tool for the first time, since it is impossible for a user to understand “facebook.com” after signing up for the first time. This point was also made by ODPC in the first report. While this helps to constitute a valid and meaningful act of consent, there must be a document in the end that specifies in one place what certain actions that are done “inline” mean and what consequences they have. This has in the end to be done in a privacy policy, which might be separated into “modules” for the different functions of facebook.com a user has activated.

Examples of incompliance

I am still of the view that (while the new policy has at least shrunk to one single document) it is still not a valid basis for the processing by FB-I. This is not only because of the vague, unclear and lengthy style, but also because many provisions seem to be in violation of the DPA and Directive 95/46/EC. I have summarized some issues as examples why I am still of the opinion that this cannot be the basis for a valid consent:

- a. I believe FB-I has to **clearly say or list what they do with my data**. While FB-I elaborates over pages about where they get data and how export or display it to users they are not saying very much about what happens in the “black box”.

Currently the only sentence that generally controls the use of user data is the following:

“We use the information we receive about you in connection with the services and features we provide to you and other users [like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use].”

This sentence splits into two segments:

The first segment defines a purpose which embraces all “*services and features*” FB-I provides. If this segment is inverted it says that FB-I is only *prohibited* from using data in relation to services and features it does *not* at all provide. In plain English this translated segment says

“We may use your data for everything, except of things we don’t do.”

The second segment defines the people in relation to which FB-I may use personal data. This segment limits FB-I's use of personal data in relation to "*you and other users*". These other users are then specified by giving examples ("*like*") which amount to everyone FB-I has any contract or business with. Given the fact that FB-I has about 1 billion users and millions of additional partners, cooperate users or advertisers and we currently have a little more than 2 billion internet users, this is again a meaningless definition and translates to the following sentence in plain English:

"We may use your data in relation to everyone we interact with."

This is maybe the most abstract (and therefore the most *unlimited* and *unspecific*) purpose ever written into a privacy policy. It can impossible be a "specific and informed" consent. This is rather a text book example of blanket consent: Practically any set of operation can be done under this provision. Such a statement is totally contrary to the law and any legal interpretation I know, including WP187, pages 19f. This sentence is so absurd and circular in nature that I usually get a round of laughs from privacy law experts when showing this phrase at conferences.

On top of this, the policy also claims that users consent to **any future developments** of Facebook. So users are supposedly giving a "specific and informed" consent to processing that does not even exist:

"Granting us this permission not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways."

There is no way that consent to an unclear and non-existing future form of processing personal data can in any way be informed or specific. This allows FB-I to do practically everything, since the limitation to process data only in relation to "services and features" as examined above can be widened any time by FB-I's decision to engage in new "services and features".

- b. FB-I has to work towards a "**modular**" policy system that allows getting an overview over the process and then consent to it. FB-I works in this direction by implementing "in line" consent, but this is currently a fractioned system, which mainly leads to confusion, not informed consent.
- c. FB-I has to implement an "**Opt-In**" instead of an "Opt-Out" system for all data use and all features (e.g. face recognition, applications or tags). Now new options are automatically activated without notice. Users should be able to make an informed decision. This is also in line with the findings of the ODPC in the first report and WP187 of the Article 29 Working Party. See also Complaint 16 below.
- d. FB-I has to precisely say **which personal data** it stores. Currently there are only very vague and general claims (e.g. "*We receive information about you from your friends and others*"). Clear information could be delivered through a continuously updated list of all data categories and subcategories that are stored about a user. FB-I should also explain the purpose for keeping the information. It has to be clear and easy to understand what is generally captured by FB-I's services.
- e. FB-I has to clarify who is responsible (the "**controller**") for what part of FB-I. I oppose that users FB-I now claims that it is the controller for personal pages, messages and pictures. FB-I has put a provision into the new policy saying it is the (sole?) controller, but at the same time FB-I makes public statements to the contrary (see "General Remarks 3: Controller" above).

- f. FB-I has to use clear and understandable language. I think that FB-I's usage of **vague wording** (e.g. "like", "may" or "could") is not appropriate for a specific and informed consent.
- g. FB-I has to rewrite the information on "**cookies**". FB-I should clearly say which kind of cookies (e.g. HTTP or Flash), with which content and for what exact purpose they are using. The current section is full of general statements: "*We use technologies like cookies ... to provide and understand a range of products and services*".
- h. After it was discovered that "deleted" information was still kept by FB-I they simply **relabelled** the buttons to "**hide**", in order to prevent people from effectively deleting data, this cannot be the proper reaction. It usually takes extra effort to really delete information (hidden sub menus) and intends to deter users from deleting data. I believe FB-I has to have "delete" as a standard option to allow user control and in order to allow users to withdraw previous consent.
- i. FB-I has to implement functions that allow users to "**mass delete**" data. Such as a function to delete all data of a certain category and all data that is older than a certain date. This allows users to efficiently get rid of old "junk data" if the users wishes so.
The reports' approach of highlighting "per item" deletion makes it practically impossible for users to delete more than just individual pieces of data. If a user wants to delete e.g. all old data on a timeline they would sit for hours to click on every item for at least three times to get rid of it.
This in fact undermines the possibility to withdraw consent for the processing of data: Users are only able to delete the whole account, or little bits of data, there is nothing between these two extremes. It is state of the art with all other "cloud" systems to allow for mass deletion.
- j. FB-I has to list **specific data retention criteria** that make it clear to users how long which information is held by FB-I. Currently FB-I just says that it may keep old information as "*long as necessary*", which is a mere restatement of Section 2(1)(c)(iv) DPA, but not an adequate information about FB-I's actual practice. The ODPC has asked FB-I to provide a clear retention policy; I am missing such a clear statement by FB-I up to this very day. In a video Erin Egan (Facebook Inc.'s "Chief Privacy Officer") was trying to explain retention periods, but only said that she "*thinks*" FB-I was talking about 180 days (see video on [YouTube](#) at 19:04), but this is about as much as I was able to find out in relation to exact retention periods. Such non-information about exact retention periods is unacceptable and does not allow for a specific and informed consent.
- k. FB-I has to take back the change that allows them to keep users' information **after users have deleted their accounts**.
It used to be that FB-I said it deleted all information when you delete an account, this was changed with the new policy. FB-I does at the same time not disclose *which* information is kept after deletion of an account and *how long* such information is kept. I ask the ODPC to find out which data is kept, the purpose for this and the legal basis for such processing. This provision also seems to be in conflict with the withdrawal of consent and the idea that data which is used on the bases of consent should not be processed on another basis when consent was withdrawn (see WP187).

- l. FB-I has to take into account that it cannot effectively enforce its policies in relation to **external developers**. As the investigations of the ODPC have shown FB-I cannot even ensure that developers have some sort of privacy policy, not to mention the other obligations of an external provider of applications. FB-I cannot rely on agreements with external contractors, if they are impossible to police and enforce in reality. FB-I points at agreements that are not worth the paper they are written on. FB-I should close these loopholes in the legal framework and find other solutions that might mean that only developers that are certified, checked or at least personally identified can get a hold of users' data (see also "Complaint 13 - Applications").
- m. I believe FB-I has to take back the change that makes the user responsible for **deleting the data from applications or other third parties**. The old policy said developers are obliged to delete all user data as soon as the user deleted the application, which was in line with the EU laws and the Safe Harbor agreement. Under the new policy the user has to specifically ask the application provider to delete such data. The deletion of an application is a clear and explicit act that constitutes a withdrawal of consent, previous consent cannot be a basis for further processing.
- n. I believe FB-I has to limit the use of users' data for advertisement and other purposes to certain data categories. Currently FB-I can use **any of the users' data for advertisement** (e.g. private messages, sexual preferences, interactions with friends or what others post and share). The new policy restates this. While FB-I is, according to the reports, claiming that it is in fact not processing all data categories for all purposes the privacy policy does not reflect this and needs to be adapted in a way that this is reflected.
- o. FB-I has to take back the changes that limit the scope of the "**show my social actions in FB-I Ads**" options. Under the old policy users could turn this function off, the new policy limits the scope of the opt-out.
- p. FB-I has to disclose which data categories are used for **determining users' personal interests**. Currently it is unclear how FB-I finds out users' interests for targeted advertisement if the information is not posted by the user (see also Complaint 02 – Shadow Profiles).
- q. FB-I uses mainly **examples** to explain their processing. Most of these examples seem reasonable (e.g. if users say they "like" cars, they get ads on cars), but the general provisions also allow for other processing that might not be that reasonable an acceptable for users. I believe that FB-I has to highlight processing that cannot be reasonably expected, instead of rather obvious processing. Everything else would be a misrepresentation of facts and lead to an invalid consent.

As said before, the issues listed above are only some examples for incompliance. In general FB-I's privacy policy has extremely vague and general provisions, that allow endless leeway. A data subject cannot predict what FB-I is, or is not doing with its data after reading this document. FB-I does provide some examples that substitute these general rules which allows for some insights, but as they are not an exhaustive description of FB-I's operations they cannot be a basis for a valid consent.

➔ ***F62: FB-I's policy is in many ways incompliant with the law and is in no way holding up to the minimal standards set out by the Article 29 Working Party.***

How far can FB-I's wording be bent?

To show this in a more practical way I also want to give the following examples on what is "allowed" under the current policy of FB-I:

- a. FB-I may collect any kind of data, including highly sensitive data. As it does not differentiate between different kinds of data it could e.g. generate a list of all people that have severe health problems (e.g. cancer or AIDS), that are sympathizing with certain political parties, that have a certain sexual orientation or a list of all people that are trade union members. FB-I just blankly says it receives any number of different types of information about users:

*"We receive a number of different types of information about you" -> **FB-I uses any Data...***

- b. FB-I may use this information not only if users have shared it, but also if it has acquired them through any "third party" (e.g. users, advertisers, data brokers, app developers, any government, the internet, other peoples' private communication). In plain English: Anyone in the World.

*"We receive information about you from your friends and others" -> **...from anyone...***

- c. FB-I grants itself the right to not only use this information of certain activities (e.g. advertisement) but allows itself to do anything with it. It e.g. could forward this data so "data brokers" use it for "credit assessment" or start a "spy on your friends feature". The wording does also not only cover activities data is necessary for, but allows anything that is "connected" with any service or feature:

*"We use the information [...] in connection with the services and features we provide to you and other[s]"
-> **...for any purpose FB-I engages in...***

- d. FB-I grants itself the right to not only use this information in its own interest, but also allows itself to use it "in connection with" anyone in the world. The phrase "other users" is only defined by a demonstrative list that does not enclose all options as it is followed by the word "like". But just the word "other users" already including more than a third of the internet (roughly 1 billion Facebook users of less than 3 billion internet users). In addition FB-I is also names "partners", "advertisers" or "websites". The wording allows using data "in connection" with anyone FB-I engages with.

*"[others] like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use." -> **...in connection with anyone it engages with.***

In summary FB-I could start a "Who's got AIDS?"- or a "Who is a bad employee"-feature tomorrow and use *any* data it can gather from *any* source in the world and then use it "in connection" with any "partner" (e.g. health insurances, employers or banks) it would like to use it with. There is no sentence in the policy that would prevent such use. Overall I was unable to think of anything FB-I could possibly do to violate its own policy, but it is drafted to allow practically anything and is therefore impossible to violate.

➔ **F63: FB-I's policy is written in a way that it can practically gather any data and process it for any purpose it wished to engage in. It might be best described as an "unviolatable spandex-policy".**

Need for “flexibility”?

FB-I sometimes claimed that the policy has to be “flexible” to allow for new services without changing the policy every time. In fact FB-I currently proposes the fourth (!) policy since I have filed my initial complaints, despite having a very “flexible” policy. So this argument seems to lack any substance. In addition there is nothing in the law that would in any way allow for an exception in such a case.

Summary: Content of “New Policy”

Overall I believe that FB-I has to draft a totally new policy. I suggest there is one section for the core features and additional sections for additional features that users consent to opting into such features. This idea of “layered notices” was also repeatedly outlined by the Article 29 WP (see e.g. WP 203).

FB-I should get rid of unclear and vague wording that in the end allows to do practically anything, as this is in no way allowing for a “specific” consent. Words like “can”, “may” or “like” are usually meaning that the following text is not legally reliable or is only explaining on part of the processing operation.

FB-I has to clarify the purpose for different kinds of data and cannot rely on one general sentence for all of its processing operations. There is no way that such a “purpose” can in any way be seen as “specific”. The WP 203 is in this respect making very clear that a much higher level of detail must be met.

FB-I should prompt users about any major updates and thereby get explicit and informed consent whenever new features are introduced. Such a system would be in line with the law as well as WP187 and WP163. Such an approach would surely be supported by NGOs, DPCs and users and would constitute real “best practice”.

The tactics of FB-I seem to be that it wants to also meet the requirements of its US parent company which is subject to the FTC. The US privacy system is however only relying on self-limitation through policies. If “Facebook Inc” is drafting a very abstract “spandex policy” it avoids any form of troubles with the FTC. This is reasonable, but is incompliant with the European legal system. It seems to me that FB-I has to liberate itself from its US parent and needs to adopt a specific policy for operations outside of the US and Canada, while its parent “Facebook Inc” may keep a defensive American “anything goes” policy.

➔ ***F64: The currently used policy is somewhat more readable than the policy which was used when the original complaint was made. However it is still way too long for any normal person to read. It is extremely vague and allows FB-I to practically conduct any processing operation it wishes to do. In every respect it does not comply with the law and the very clear minimal standards set out by the Article 29 Working Party.***

➔ ***F65: FB-I and “Facebook Inc” are operating in two different legal environments. The EU is requiring specific and clear information - unlike the US. To match this difference FB-I will need to have a separate policy for operation under Irish/EU law. The “Facebook Group” cannot pick and choose some laws from the US and some from the EU. Each separate entity must respect all local laws.***

Act of Consent

Old Sign-Up Process

I welcome that the ODPC has made FB-I change its sign-up process towards a new system that gets much closer to what I have outlined in my initial complaint (see blow). At the same time the report does not say one word about the millions of users that have signed up to facebook.com before this change was made. There is no mentioning about the validity of the consent for former users. If the ODPC is saying that the form of consent that FB-I obtained previously is not satisfactory, there is no stringent way around that this means that users that signed up previously have not given a valid consent. I am still of the view, that FB-I does currently not have a valid consent by users that signed up before this change. However this still allows FB-I to operate under other provisions of the DPA and Directive 95/46/EC (e.g. performance a contract).

FB-I is cited repeatedly in the report from December 2011 to claim that the ongoing use of facebook.com would constitute informed, specific and unambiguous consent to the (old or new) policy. I am again pointing to WP187, which is clearly saying that the sole use of a page (or online game) does not constitute unambiguous consent to a far reaching privacy policy (see WP187, page 23).

→ ***F66: Old users have still not given a clear consent. The claim that the “continuous use of the page” would constitute “informed, specific and unambiguous” consent is simply false.***

New Sign-Up Process

I welcome the improvements, but the new page is still not really emphasizing that there is some act of consent to a privacy policy. The relevant text has grown by only 1 pixel (!) from 7 to 8 pixels, making it again the smallest text on the page. All other text is at least 50% bigger (13 pixels).

The screenshot shows the Facebook sign-up page. Red arrows point to various text elements with their pixel sizes:

- 27 px**: Points to the "Sign Up" heading.
- 13 px**: Points to the "Your Email" input field.
- 13 px**: Points to the "Month" dropdown in the "Birthday" section.
- 15 px**: Points to the "Sign Up" button.
- 8 px**: Points to the small text: "By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use."

The page includes a login section at the top right, a sign-up form with fields for First Name, Last Name, Email, Re-enter Email, New Password, and Birthday (Month, Day, Year), and radio buttons for Gender (Female, Male). It also features a "Sign Up" button and a link to "Create a Page for a celebrity, band or business."

Screenshot: New sign up page on facebook.com with size of different text.

I still question if this small link can really constitute an informed and specific consent, given the large amount of very problematic and complicated data processing FB-I engages in. Nobody in the world could argue that anyone that clicks this button has read (for 45 minutes) the policy behind this link and is therefore giving a “specific and informed” consent.

The reports did also not take into account the fact that facebook.com has become a standard form of communication and that a consent to a monopoly is hardly “free”. This view was also shared by the Article 29 Working Party in WP187:

“Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioral advertising in order to avoid the risk of being partially excluded from social interactions.”

The solution is at the same time surely a step ahead concerning the sign up process to ensure a less “ambiguous” consent. “Best practice” would be at least a check box, which is seen to be necessary for any form of consent in many member states, however I can see that this element of a valid consent may now be met given the more tolerant interpretation of the law in Ireland.

- ➔ ***F67: The new sign-up page is a step in the right direction, but hardly in line with the law and for sure not “best practice”.***
- ➔ ***F68: The relative size of the text was practically not improved, there is no “check-box” and the consent to the usage of data is not separated from consent to the civil law terms. However the new version might constitute at least an “unambiguous” act of consent.***
- ➔ ***F69: The DPC did not touch on how “free” consent on facebook.com really is. FB-I did bring forward any counterarguments in relation to this matter.***

Improved Information for new Users

I welcome that new users get additional information. At the same time new users are still not “walked” through the settings, but there is only one of many links to this information, which appears on the “Welcome Page”. The four steps are not taking into account all the different settings FB-I offers, but only show some settings that are already well known to many users. Every information constitutes of a picture and only one or two sentences:

1. “You can pick and choose the audience for the things you post on your timeline — like share your school publicly, but only let friends see your photos. You can also hide the things other people post to your timeline.”
2. “~~Tagging is an easy way to let people know when they're in photos*~~. A tag creates a link to the person's timeline and may share your post with their friends.”
3. “You can control who can send you friend requests in your How You Connect settings”
4. “Control who can access what, including what info your friends and others can bring with them in the apps and websites they use.”

I am wondering how these 107 words (of which 14 words are only promoting a tool) can constitute proper information about a highly complex system with more than 170 possible options (*counted by the "New York Times" in 2010*). Many options are not explained at all. There is e.g. no mentioning that users can totally turn off "apps" or "personalized ads" or the options for the access by search engines. If this information is compared with the more than 9.300 words of the privacy policy one can be sure that this does not ensure proper information.

→ ***F70: The additional information that is provided is another small step into the right direction, but surely not the giant leap towards an informed consent by all users. In fact this seems to be more of a "placebo" so that FB-I can claim it has done "something".***

I still believe that only a system where users get a quick information when they first use a function compared with "privacy friendly" default settings can combined constitute a specific, informed and unambiguous consent.

C. Additional Submission of Facts:

I also want to mention the issue of "withdrawal" of consent. This was not explicitly covered in these complaints, even though I have touched upon the topic repeatedly in other complaints. FB-I is however making it currently impossible to take back the consent for most data. It is either impossible to delete such data (e.g. removed friends) or it is practically impossible to do so (e.g. every "event", "like" or old "post" must be deleted individually). By designing the software in such a way FB-I is making it factually impossible to withdraw consent.

F71: FB-I has designed its system in a way that users cannot withdraw consent in any way.

D. Legal Consequences described in the Original Complaint:

After analyzing this circumstance, I think that Facebook Ireland does not have the right to use personal data of its users according to its privacy policy, since there is no consent that is in any way effective under section 2A(1)(a) DPA or Article 7(a) of the Directive 95/46/EC.

Facebook Ireland may continue to process some personal data because of the performance of the contract with the user, as defined in section 2A(1)(b)(i) DPA and Article 7(b) of Directive 95/46/EC. This limits Facebook Ireland's ability to use personal user data to the mere hosting of the users data. Any other processing of personal data could only be done after all users consented to a privacy policy that fulfills Irish and European standards.

E. Additional Statement on the Legal Consequences:

In addition to the original statement and the points made above I also want to draw the DPC's attention to the relevant Working Papers by the Article 29 Working Group (e.g. WP 163, WP 187 and WP 203), which are further specifying the issues I brought up. I understand that the DPC is taking these European minimal standards into account when deciding about my complaint.

Withdrawal of Consent

Overall the free consent must be given when data is put into a system, but must also be upheld for further processing. In addition FB-I is generally granting users the possibility to remove content.

In relation to processing is not done by the user as controller it is part of the "informed" consent, that things can also be removed if a user is unhappy with it. This view is also reflected in the WP 187 (page 33 and 34) which is clearly saying that any further processing has to be stopped after a user has taken back his consent. Whenever the user is the controller the possibility to "remove" data is directly following from the duties of the processor (see complaint 18 below).

- ➔ ***R34: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above and is also continuing to do so today. I also ask the DPC to prevent such processing.***
- ➔ ***R35: If the DPC is departing from the common understanding within the EU on these matters I am hereby asking the DPC to explain why he does so.***

12.Complaint 09 “Face Recognition”

A. Facts described in the Original Complaint:

Facebook Ireland started to analyze photos that users were tagged. The product of this analyzing process is biometrical information that is stored by Facebook Ireland.

According to Facebook Ireland the sole purpose of this generated data is to suggest to users people they could tag in pictures they upload. This means that instead of having to type in a name Facebook Ireland is suggesting a person and the user has to say yes/no. This saves the user that wants to tag another person a couple of key strokes, since before that he/she had to first click on a part of the picture and then enter the first couple of letters of the person’s name in order to find the person.

The mere existence of such data bears tremendous privacy risks, since this could enable the holder of the data to analyze live information (e.g. CCTV) or to analyze information on the internet or by using cell phones. Public authorities may demand access to this information for their purposes.

Facebook Ireland is indicating its use of photos in its privacy policy, but not in the general explanation about privacy that users see when they click on “privacy” on facebook.com. Within the 12 pages (!) of the privacy policy the following two (!) sentences clarify the use:

“Similarly, if one of your friends uploads a picture of you, we may suggest that your friend tag you in the picture. We do this by comparing your friend’s pictures to information we’ve put together from the photos you’ve been tagged in” (see attachment 03).

Facebook Ireland is not clearly saying that it generates biometrical data of every individual user and is avoiding the term “face recognition”.

This provision is new and users that signed up to facebook.com years ago might not have agreed to this provision at all. The users are not asked to agree to changes in the policy after they were changed. This would be really easy by simply having a prompt when users log on to facebook.com.

The new feature was automatically activated without the prior specific information of the user. Users did not get any information (like e.g. a prompt after logging on) by Facebook Ireland about the activation of this new and very intrusive feature.

It is rather hard to deactivate the feature. It takes at least 7 clicks from the front page, some links are rather small and are hard to find. Users without good internet skills might not even find the appropriate buttons (see attachment 04). The user is only informed about the benefits of this function. This might be manipulating the free will of the data subject. The data subject is by far not “informed” in a balanced or neutral way.

Even if the user deactivated the function, the user’s tags are still used. Only after visiting the help center on facebook.com the user finds out, that it he/she deactivated the feature, the biometrical data is still saved (see attachment 05). According to the help center information the user has to click on another button to actually delete the biometrical data that was generated. When I tried to do so, there was no button on the page described (see attachment 06)

B. Reaction by FB-I and the DPC and Additional Facts:

I very much welcome the deactivation of the automatic biometric facial recognition tool (called “tag suggest” by FB-I). The tool was clearly not in line with the DPA and Directive 95/46/EC. This was very clearly stated in WP163 issues by the Article 29 Working Party. The procedure has shown to my understanding, that there must be unambiguous, informed and specific consent for additional processing like the facial recognition. This cannot be obtained by inactivity of the user or by an “opt-out” system (see also WP187, page 35). I hope the ODPC is moving towards this - European - understanding in relation to other complaints as well (e.g. Complaint 16 – “Opt Out”).

What is at the same time disturbing is that the ODPC has in the relating statements more or less said that an unambiguous consent is not really necessary under the law, but more a consequence of pressure from other European DPCs and somewhat inspired by the ODPC’s “best practice” approach.

I also want stress that the ODPC has not dealt with the other provisions of the Irish DPA and Directive 95/46/EC that are necessary to make this form of data processing legitimate. The Article 29 Working Party has clearly stated that even a valid consent does not allow the controller to waive other principles of data protection law (see e.g. WP187 page 34). Especially the requirement to be non-excessive seems to be relevant in the relation to FB-I’s facial recognition tool. The ODPC has not at all elaborated the question whether it is proportionate to generate biometrical data of 1 Billion users only in order to avoid a couple of clicks for a user that wants to tag someone. It his is not excessive, I wonder what is?

Even though the first attempt by FB-I to get the tool “approved” by a notice on facebook.com seems to be obsolete after the Re-Audit, I still want to quickly point to the wording and the way FB-I has implemented this mechanism. The following information was displayed to users:



Wording used by FB-I (Screenshot delivery by Richard Allan, FB-I).

Despite the fact that the message was only displayed three times and the user was further enrolled with the facial recognition tool if he/she was not interacting with it (see above) the wording not allowing for an “informed” consent. There is no word on “facial recognition” or “biometrics”. By the wording FB-I only uses the information that someone is “tagged” (so the tag information itself) to group pictures. In reality FB-I uses their faces (*not the tags*) to do so. The wording of the button (“Okay, Got It”) does not give the impression that the user has a choice, but that this is just an information. Further information and an option to turn the feature off, could only be found in the second or third layer of the menu. Color, pictures of friends and vague wording was also used to deter users from opting-out. All together is a prime example how there would never be a valid consent, even if the user clicked on “Okay, Got it”.

New System(s)

FB-I has pledged to turn off “tag suggest” in the EU/EEA after the “report” in September 2012. In fact “Facebook” has turned the feature off in the whole world. On January 31st 2013 it has now said that it has turned it back on for “users in the United States”.

FB-I has not given any statement as to how this is technically separated. If a user is uploading a picture of a European citizen in the United States it seems to be difficult to have a “clear cut”. From a logical side it seems to be necessary to recognize people first before it can be checked if they have consented to facial recognition or if they are living outside of the US/Canada – and are therefore subject to EU laws.

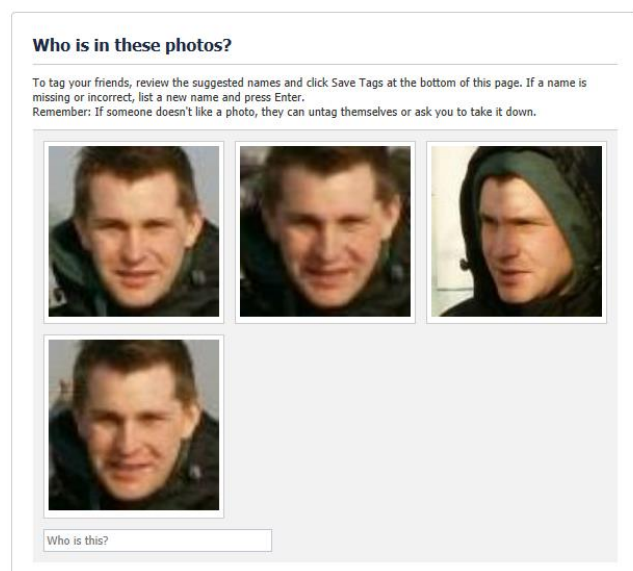
“EU” and “EEA” are also the key words for the last remark I want to make: According to the reports the ODPC is responsible for all processing of “Facebook Ireland Ltd”, so all operations of facebook.com outside of the US and Canada. The DPA and Directive 95/46/EC do not distinguish between the data of “EU data subjects” and the data of other people.

It is therefore not stringent, that FB-I was only made to comply with the legal requirements for users’ “within the EU/EEA”. The right to data protection is not only a human right (in opposition to “citizens’ rights”) but I am also bound to protect the right to data protection of users’ outside of the EU/EEA according to international law. Any user from associated countries (like e.g. Switzerland) will hardly understand why the ODPC did not enforce their fundamental rights.

- ➔ ***F72: It is unclear how the “Facebook Group” (FB-I and “Facebook Inc”) is able to distinguish between US and non-US data subjects without first having everyone go through facial recognition.***
- ➔ ***F73: FB-I is responsible for anyone outside of the US/Canada. Therefore it does not make any sense that the DPC has ordered FB-I to only delete data of EU/EEA users. Instead the data of all users outside of the US/Canada should have been deleted.***

FB-I has now again stated to “group” pictures based on facial recognition. It does not explain how this is in line with the recommendation of the DPC. In any event it seems like FB-I has only stopped to produce templates of users in the EU/EEA, but is still processing every uploaded picture via a “facial recognition” function that at least generates an “ad hoc” template.

- ➔ ***F74: FB-I is again using “facial recognition” at least on a “ad hoc” basis for all uploaded pictures and is at least using it to “group” pictures what it thinks to be the same person.***



Screenshot: “Facial Recognition” used to group newly uploaded pictures.

The only information that FB-I is currently giving is the following statement in its privacy policy. It has in no way been changed after FB-I has stopped “facial recognition” in the EU/EEA:

“We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from the other photos you've been tagged in. This allows us to make these suggestions. You can control whether we suggest that another user tag you in a photo using the “How Tags work” settings.”

This is describing the “matching” between new pictures and previously generated templates, but is in no way saying that FB-I may also just “group” pictures that are newly uploaded. There is also no option to turn this off – in contrast to what the privacy policy says. FB-I is currently showing users (at least in Austria) that this feature is “unavailable”, despite the fact that it is “grouping” people through “facial recognition”. Overall there is no form of consent to this process, as the currently used process is not described in the privacy policy and there is not even a way to “opt-out” of this processing – despite what the privacy policy says.

How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	Off	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

Screenshot: “Facial Recognition” is “unavailable”

➔ **F75: There is no proper information about this “limited” facial recognition. There is no consent and not even any form of “opt-out” from this form of processing.**

C. Legal Consequences described in the Original Complaint:

1. *It seems that there has never been a specific, informed and unambiguous consent by the user to the face recognition program. The function was activated automatically, and the biometrical data generated without a possibility for the user to object beforehand. The processing of data is therefore illegitimate under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*
2. *Gathering biometrical information of about 750 million users, of which about 500 million have a contract with Facebook Ireland (all users outside of the USA and Canada), seems to be excessive in comparison to the purpose. Highly sensitive data with a high risk of misuse is generated to save the user a couple of key strokes to enter a name. This form of processing personal data is clearly excessive in comparison to the purpose as specified in section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*

3. *There is no transparent notice that the generated biometrical data is still held after the function is disabled. This breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*
 4. *There is no information in Facebook Ireland's privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.*
 5. *There is no longer a legitimate purpose for holding on to the biometrical data after the user has deactivated the function. There is no other purpose specified by Facebook Ireland. The data would have to be deleted according to section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
 6. *After the user has deactivated the function, any further processing of the biometrical data is no longer relevant for the purpose of the processing and seems to be also excessive, which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
- ➔ ***R36: I hereby – involuntarily – ask the DPC to find that FB-I has violated the sections of the law listed above.***
- ➔ ***R37: If the DPC is departing from the common understanding within the EU on these matters I am hereby asking the DPC to explain why he does so.***

D. Additional Statement on the Legal Consequences of the “new” System:

1. It seems that there has never been a specific, informed and unambiguous consent by the user to the face recognition program. The processing of data is therefore illegitimate under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.
 2. Gathering biometrical information seems to be excessive in comparison to the purpose. Highly sensitive data with a high risk of misuse is generated to save the user a couple of key strokes to enter a name. This form of processing personal data is excessive in comparison to the purpose as specified in section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.
 3. There is no information in Facebook Ireland's privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.
- ➔ ***R38: I hereby – involuntarily – ask the DPC to find that FB-I is continuing to violate the law through the new “facial recognition” system. I ask the DPC to prevent such processing.***
- ➔ ***R39: If the DPC is departing from the common understanding within the EU on these matters I am hereby asking the DPC to explain why he does so.***

13. Complaint 10 “Access Requests”

One of the most “prominent” complaints was the complaint dealing with the right to access and FB-I’s non-compliance with my initial access request that was sent to FB-I on June 2nd 2011. Given the fact of its prominence and that more than 40.000 people have made access requests as well I would have expected that this issue would be prioritized and investigated in an especially transparent and detailed way. Instead I had to find that the exact opposite has happened, which is also supported by the facts I had to find when looking at the current “solution” to access requests.

A. Facts described in the Original Complaint:

I have tried to get full access to all my personal data that is held by Facebook Ireland. This took a multitude of e-mails and a first complaint with the DPC in Ireland (see attachment 02a). I also sent a list of data of which I would like to have a copy (see attachment 03). Facebook Ireland first sent me a PDF file with only limited data (see attachment 04) and later sent me a CD with another PDF file with 1.222 pages (see compressed version in attachment 05). This CD was sent via airmail by Facebook USA. Even after Facebook Ireland sent me this CD, there is personal data that was not disclosed to me by Facebook Ireland. This includes the following information:

1. *Content I was posting on other peoples sites (see e.g. attachment 06, page 10)*
2. *Information in connection with the 15 videos I have posted on Facebook*
3. *The information that I “liked” certain content all over the Facebook platform*
4. *Information about my browser type, as listed in Facebook’s privacy policy (attachment 07)*
5. *Information about my interaction with advertisements (as listed in the privacy policy)*
6. *Information gathered through “conversation tracking” (as listed in the privacy policy)*
7. *Information that “indicates a relationship” with other users (as listed in the privacy policy)*
8. *Information about pictures that I used to be tagged in, but removed my tag from.*
This “tag”-information is still saved, since the Facebook platform does not allow other users to tag me again in pictures from which I “untagged” myself (see attachment 09).
9. *“Tracking information” that Facebook Ireland gathered from my use of other websites, such as when I clicked on a “like”-Button, or just loaded the plug-ins from Facebook by visiting some website that implemented plug-ins from Facebook (as listed in the privacy policy).*
10. *Information about “Searches” that I made through the “search” function.*
11. *Information about settings such as the newsfeed settings (see attachment 08)*
12. *Information about “click flows” and the visits of individual pages of the platform (as listed in the privacy policy)*
13. *Information about the use of my personal data in the “friend finder” functionality of the Facebook platform.*
14. *A disclosure about the use and outcome of any processing of my data, such as “matching” processes, face recognition or targeting for advertisement.*

15. Information about the use of my pictures for Facebook Ireland's new "face recognition" tool, or the outcome of such a process (such as biometrical data that may be used to identify me).
16. Data that Facebook Ireland gathered about me (e.g. my phone number) when other people "synchronized" a device (e.g. iPhone) with Facebook. I know about at least one person that uploaded my phone number.
17. More detailed information about my relationship to other users. Facebook Ireland is e.g. asking users where they know each other from and they track how often users interact on facebook.com. This information was not disclosed.
18. Information on individual content I was posting that indicates the reaction of other users. On Facebook Ireland's "Pages" the user can see these indicators right on his wall.
19. Information about "invitations" to groups, events or pages I sent to other users or other users sent to me.

It is very likely that Facebook Ireland holds much more than this list. From different data requests by two different friends of mine it was obvious that Facebook Ireland sent different categories of data to each one of us.

Besides this, Facebook Ireland only supplied the raw data to me. This happened without description of used codes like "NS_SUCCESSFUL_VETTED" as information saved with every login I made or the information that "tags" in pictures have an "active" status, which raises the question about "inactive" tags. There are many data fields that are not self-explanatory and need some kind of explanation (see attachment 05).

Facebook Ireland did also not provide any information listed in section 4(1)(a)(ii)(III) and (IV) DPA, even though I asked two more times for the purpose and the recipients (see e-mail from the 15th of July and the 18th of July 2011 in attachment 02). In two e-mails sent on the 18th and 19th of July 2011 Facebook Ireland repeated that they do not have any such information.

Facebook Ireland also did not name the source of the data as necessary under section 4(1)(a)(iii)(II) DPA. For example there has been an e-mail-address associated with me that never really existed [REDACTED] and Facebook Ireland could not name the source of this information. Many of my friends are using "applications" which made it possible to have my personal data transferred to the developer of this application. Facebook Ireland could not give me any details about any such flow of data.

B. Reaction by FB-I and the DPC:

Despite the fact that the “access requests” were a point of great public discussion with more than 40.000 users directly affected and about 1.000 complaints at the ODPC there is very little information that can be derived from the reports.

Exceptional “hardship” on FB-I through Access Requests?

The report starts out to claim that the 40.000 requests were a massive issue for FB-I and that this “*would place a strain on the ability of any organization to provide personal data within 40 days.*” This seems to be rather absurd: 40.000 requests at a user base of about 900 Million users means that only 0.004% (!) of Facebook’s user base has made an access request. This is equivalent to a single request at a data controller with 22.500 costumers. If this is seen as “too much”, FB-I should not have waived the right to ask for € 6.35. It seems hypocritical to first tear down the only limitation - to then complain about an “extreme” number of requests. I believe that FB-I was simply unwilling to additionally process the payments by thousands of users and therefore waived the fee in its very own interest.

While the report was repeating the law, saying that there is no exception form the 40 days deadline under Section 4 DPA, the ODPC has in fact simply “waived” the law for FB-I. By doing so it has deprived 40.000 data subjects, including myself, of their right to access within a reasonable time. Also other controllers in the EU will have a hard time understanding why the law applies to everyone but FB-I. As communicated to the ODPC before, I am deeply disturbed that the law was simply “waived” for a tech giant. If laws are simply waived for some, this questions core values of the democratic system. This could be interpreted that the “rule of law” is not of relevance for the ODPC.

- ➔ ***F76: Access Requests by (only) 0.004% of the overall user base is not exceptional. FB-I has added to getting more requests by waiving the fee of € 6.35. There is no “pity bonus” if a controller is getting a larger number of access requests that would in any way “waive” the law for such a controller.***
- ➔ ***F77: The ODPC has illegally “waived” a statutory obligation of FB-I and allowed it to break the law.***

Fact-finding Missing

The first report states that “*a significant proportion of the audit was ... focused on establishing the extent of personal data held by FB-I and whether any of the limited exemptions contained within the Data Protection Acts could be validly claimed by FB-I.*” While the ODPC seemed to have worked through the list in my complaint (“10 – Access Request”), the ODPC has not made any evidence, argumentation or legal analysis public. There is no word on other data categories. I have no possibility to independently verify the final results (which is in fact just a tiny list). Neither the factual basis (e.g. a list of all data FB-I holds) neither the legal argumentation (e.g. which data is not “personal data”) was disclosed.

- ➔ ***R40: I ask the DPC to – urgently - disclose evidence, arguments and files in relation to the existence and legal qualification of (personal) data on FB-I’s systems.***
- ➔ ***R41: In addition I – urgently – ask the DPC to disclose the methodology of ensuring if FB-I is processing data and if it falls under the right to access.***

Doubts about FB-I's Disclosures and the DPC's Findings

As a user it is practically impossible to know about all the data categories that a controller holds, therefore the user is dependent on the investigations of the authorities to ensure that all data is disclosed. I have submitted a list of examples that should have triggered reasonable doubt about FB-I's compliance with the law. At the same time there are no facts that would indicate that the ODPC has looked for data categories beyond the list I have submitted.

The ODPC has let me know that it has taken account of the 19 data categories I have listed in my initial complaint. I have repeatedly pointed out that this was not an exhaustive list of data categories and that I expected the ODPC to investigate into other data as well. I have even offered to submit a second list of data categories that I have collected after the initial complaints. The ODPC has not gotten back to me on this proposal.

During our talks with FB-I in Vienna, the representatives of FB-I have declared that the 19 categories I listed were exactly the only 19 categories FB-I did so far not disclose. Given the fact that the list was only an educated guess, it would be an incredible miracle if I would have made a "100% hit".

In a "live session" FB-I's Chief Privacy Officer, Erin Egan has indirectly stated that FB-I does currently *not* deliver all personal data through its self-service tools (see [YouTube](#) at 21:50):

"I know people might say: 'Oh why aren't you giving us access to more'. But think about how much I am giving access to – I think it is a terrific tool and I am constantly working. You know it's not easy!"

Therefore I got very reasonable doubt that the ODPC has found all data categories. I am sure that the data categories listed on pages 64-65 of the first report do not represent *all* personal data held by FB-I.

➔ ***F78: There is very reasonable doubt that the list of data, published in the ODPC's reports, is incomplete. Neither FB-I nor the DPC has in any way provided fact based evidence about the data that is held by FB-I.***

"Headlines Only" Approach

The list of these categories is also only naming the "headlines" of the categories. It is unclear which exact data fields or sub-categories are included under these headline. The ODPC has failed to list any details about the data that is or is not included.

The report lists e.g. "photos" - but there are also IPs, dates, EXIF data or "tag" data attached to photos. These details are not listed in the report, which means that the scope of the disclosure is totally unclear.

➔ ***F79: The ODPC has in no way defined what is included in the "list" published in the report.***

Obvious Failure: “Self Service” Approach

The ODPC has repeatedly said that it has worked together with FB-I very closely and checked on the implementation and functioning of the “self-service approach” taken by FB-I. Given the obvious flaws that I discovered and described below (see section “Self-Service Approach” below) I am wondering how the ODPC could overlook these issues. It seems like the ODPC has never investigated and cross-checked on the factual implementation by FB-I. If these most obvious issues were not effectively discovered, I am very much worrying about the quality of the investigation into other issues (e.g. the investigation on other, so far non-disclosed data categories).

➔ ***F80: The ODPC has “overlooked” the most obvious inconsistencies. There is probable cause to believe that the ODPC has never properly established the facts and has not undertaken a critical and credible investigation of this matter.***

Facebook’s Credibility relating to Access Requests

In order to demonstrate that FB-I has so far repeatedly lied and made obvious false claims I want to copy four of the many emails FB-I has sent to me and other users in the past year. It later turned out that the following claims and responses were simply false, misleading and deliberate lies.

E-Mail from the June 9th 2011 in response to the initial access request

Hi Max,
We received your request for information about your personal data. Attached to this email, please find a copy of the personal data you requested.
(...)
Please let us know if you have any additional questions.

Thanks,
R#####

This e-mail was accompanied by a PDF file of **18 pages** and **5 (!)** data categories: “E-Mails”, “Locale”, “Logins”, “Name” and “Registration Date”. Soon later FB-I has given up its position and sent a PDF file with **57** data categories and **1.222 pages**.

➔ ***FB-I has lied for the first time.***

➔ ***FB-I has only given out 1.5% of the data (if counted by pages).***

Further e-mail in response to the initial access requests from July 18th 2011

Hi Maximilian,

Thank you for your email. The data included in the file you received is all the personal data we hold. If no data related to a category you listed has been provided, that means we do not have such data.

*Thanks for contacting Facebook,
R#####*

This email was sent after receiving the CD with a PDF that held 57 data categories and 1.222 pages. Later in this proceeding (and thanks to the investigation by the ODPC) it turned out that FB-I was holding many more data categories.

- ➔ ***FB-I has lied for the second time in relation to the access request***
- ➔ ***FB-I has again only given out a small part of the overall data.***

Further e-mail in response to the initial access requests from September 28th 2011

(...)

"To date, we have disclosed all personal data to which you are entitled pursuant to Section 4 of the Irish Data Protection Acts 1988 and 2003 (the Acts)."

(...)

This email was sent after receiving the CD with a PDF that held 57 data categories and 1.222 pages. Later in this proceeding (and thanks to the investigation by the ODPC) it turned out that FB-I was holding many more data categories.

- ➔ ***FB-I has lied for the third time in relation to the initial access request.***

Standard e-mail to users that made access requests, autumn 2011

(...)

"We have built a convenient self-service tool to offer people who use Facebook the opportunity to access the personal data we hold about them in accordance with the provisions of EU Directive 95/46/EC.

By offering this tool I am able to give you immediate access to your data at any time free of charge. We have included all the data that we believe necessary to comply with the requirements of data protection law in this download"

(...)

At this time the "Download Tool" offered only 22 data categories, compared to the 57 categories has delivered by to me in July 2011. More than 40.000 users have made an access request at this time.

- ➔ ***FB-I has continued to lie to more than 40.000 users. FB-I tried to make more than 40.000 users believe that only 38% of the previously disclosed data categories existed.***

Summary: Facebook's Credibility relating to Access Requests

Given this record there is no reason why I would possibly believe the current claims by FB-I that it discloses all information. After misusing the trust of users it is now upon FB-I to demonstrate by the use of solid evidence that every little bit of information that falls under the right to access is disclosed.

→ ***F81: There is no reason to believe claims by FB-I on the existence of certain data categories without solid proof, given this history of false claims and deliberate lies.***

“Self-Service” Approach

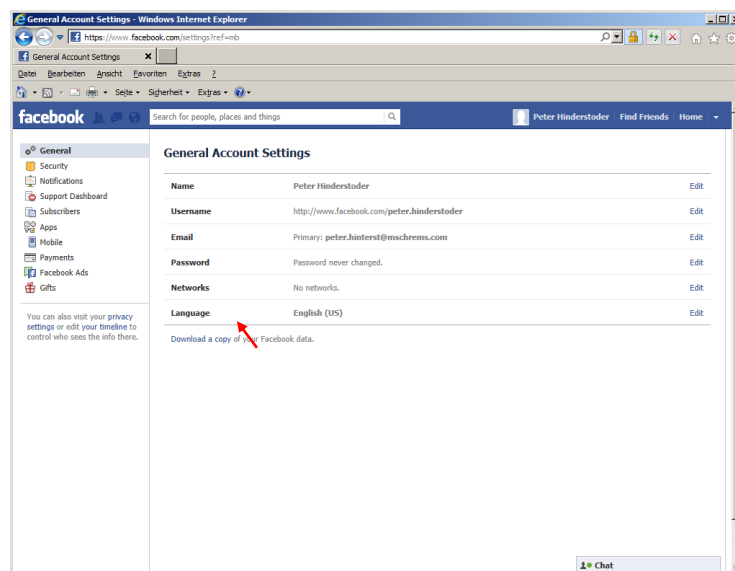
FB-I has taken a very “different” approach in relation to the response to access requests. Instead of supplying the users’ with a copy of the raw data, which is the standard procedure, the ODPC has given FB-I excessive amounts of time (more than one year, instead of 40 days under the law) to develop “self-service tools” that should allow users to access all data that is covered by the right to access. I have been very critical of this approach, since these tools replaced the standard response.

I would not have criticized this approach as an “additional” feature for users that do not want to go through the trouble of making a formal request and want to avoid the Irish “access request fee” of € 6.35, but I cannot see how such a tool can replace a formal response to an access request.

In relation to the timeframe FB-I has added the last bits (EFIX data) to the tool in October 2012, so more than a year after the initial complaints, about 1,5 years after the initial requests and 4 months after the July 2012 deadline that was agreed on in the first report, which was published in December 2011.

Download Tool(s) – Access

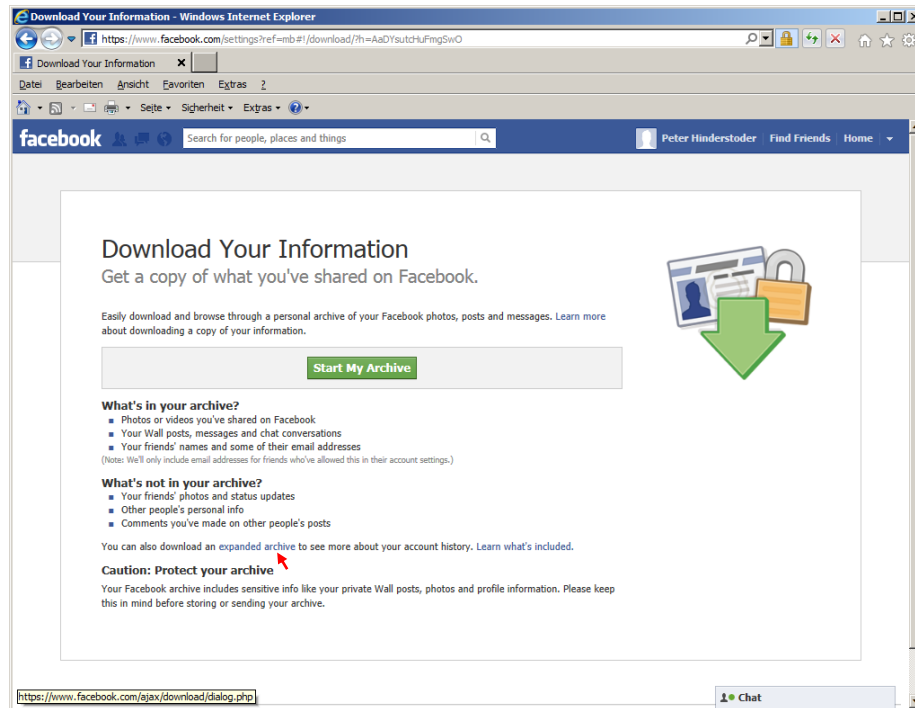
I am not opposing a “download tool” as an additional or alternative option for users to get their data in an unbureaucratic way and without costs. The tool is very hard to find: On “account setting” page FB-I has not placed a link in line with other text, but in a gray small (8 pixel) text at the bottom of the page.



Screenshot: Little gray link to the “download tool”

“Extended Download Tool” / Usability of Tools

In addition I had to find that the “juicy” information was hidden in the “extended download tool” that can only be found when clicking on a tiny link below the main “download tool”. The link was only in the 10th (!) line of text below the main tool. This separation seemed to have no other purpose than to massively hinder users to get the more problematic data in the “extended download tool”.



Screenshot: Little link to the “expanded download tool”

FB-I has even moved data that was previously available in the normal “download tool” to the “extended download tool”. It left me with the impression that FB-I is ashamed of all the data it collects instead of working towards full transparency. Only very recently FB-I has come to its senses and has moved all data into on “download tool”. At the same time data is still separated between the “Activity Log”, the “Download Tool” and other places on facebook.com

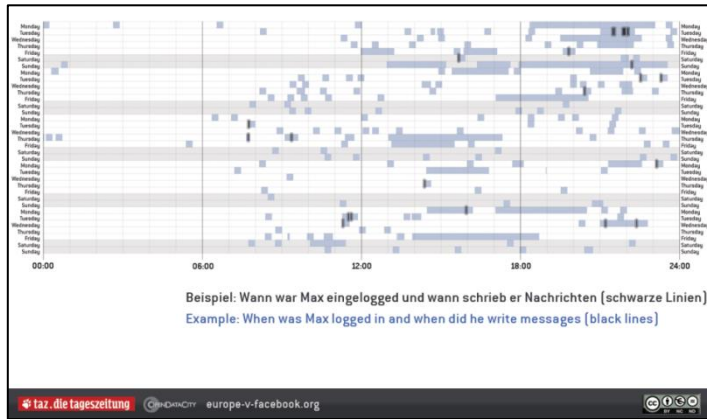
Especially inexperienced or older users might not be able to find and operate these self-service tools. Users have to make a request through the help page, they get an e-mail back, have to find the tiny links, request the archive, download the ZIP file (extract the HTML files and open them) or click through the “Activity Log”.

It takes 5 (!) Minutes of constant “scrolling” (one has to change hands) to load the whole “Activity Log”. Then I had to search and click on “See more”-Links for more than 50 (!) times to load additional individual items – taking another 10 Minutes. There is also no tangible form of the “Activity Log”. Just “marking” it from the beginning to the end in order to copy/paste it to a document takes another 5 Minutes. Overall a user will need to work for at least 20 Minutes to get data in a tangible format.

➔ **F82: FB-I makes it very hard to access the tools. Especially the “Activity Log” is not allowing seeing all data with reasonable effort and is not “tangible” in any way.**

Download Tool(s) – Content

I have found many inconsistencies when the downloaded data was compared with the “raw data” I have received previously. When comparing all three “raw” data sets with the results of today’s data sets, I was missing (among other data) much of the “meta data” associated with the users’ data.



In fact there was “meta data” to just about every piece of information in the raw data sets. This starts with user IDs, that are by definition “personal data” and associated with just about every action a user takes, goes on with exact IP addresses, URLs, dates and times, Object IDs and many other forms of meta data, that constitute “personal data”, as you can see in the picture on the left, which shows when users are “active”.

Information about the user that can be derived from “meta data”

➔ **F83: Much of the additional “meta data” is not included in the “download tool”, despite the fact that such data is clearly “personal data”.**

Deleted messages or removed “tags” - categories of data that are especially problematic, are not at all included in the download tool(s). There is no doubt that FB-I holds such information in a form that constitutes personal data. The first report only lists “inbox messages”. I was unable to find any word on why messages that were deleted, but still held by FB-I should not fall under the right to access. However the DPC has sent emails to other data subjects claiming that it would be “inappropriate” to hand out such data, which is in no way stringent. The core idea of an “access request” is to know what data is held by a company that is not visible or accessible to the user. There is also no legitimate interest in privacy by the other parties of a conversation as these messages are known to anyone taking part in a conversation. There is nothing that would be disclosed that is not already known to the requester.

➔ **F84: Practically all “removed” data is not included in the “download tool”.**

➔ **R39: Only if the DPC is taking the position that “deleted messages” are not to be disclosed I hereby – involuntary – ask the DPC hat FB-I has broken this obligation when giving me such data in 2011.**

I also had to experience that data was not showing up in the download file: As one example the “Alternative Name” category was empty in the file, even though it was visible in the “account settings”. In the current version of the “download tool” just some of my “former names” were showing up. Categories like “last location” are totally missing. This means that also categories where there is no doubt about their existence and no reason that these should not be disclosed are obviously missing.

➔ **F85: Much of the data known to be existent from my 1.222 page PDF from 2011 are not included in the “download tool”.**

In addition I have to stress, that the download tool(s) are a form of derivative data from the original raw data set. This allows for easy manipulation or technical bugs, which in the end undermines the right to access by users. I would have never been able to uncover the misconduct by FB-I without access to the raw data sets. I therefore believe that FB-I has a vital interest not to deliver the raw data.

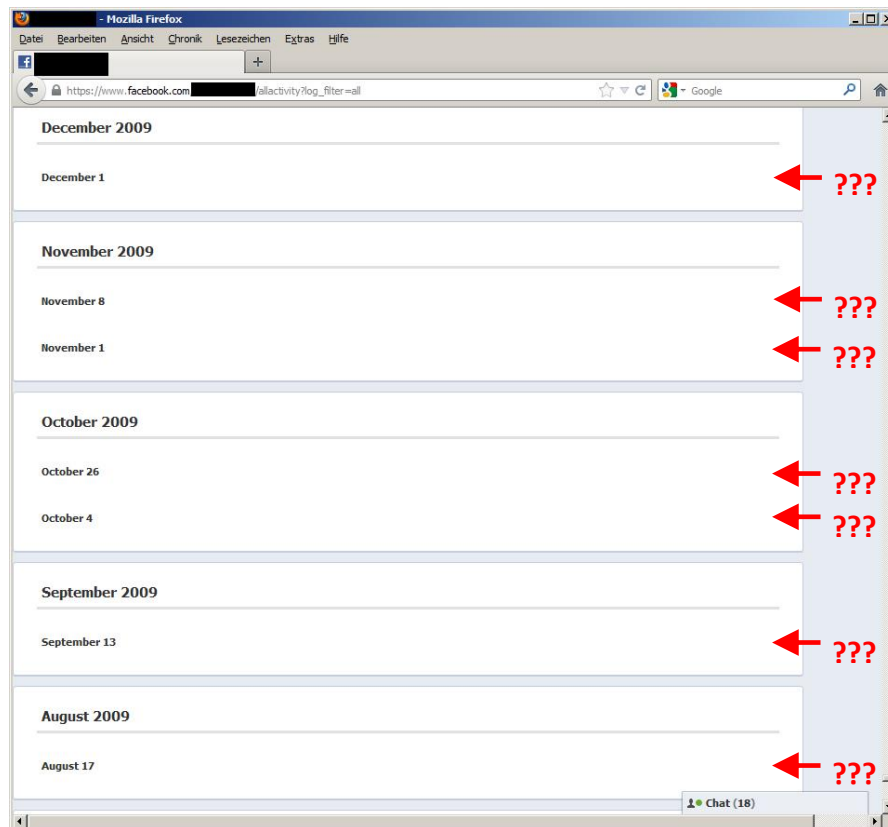
➔ **F86: By not giving a 1:1 (“raw”) copy of the original data – as stored on the servers – the core idea of the “access request” is undermined. FB-I can without any problem manipulate the content of the “download tool”. Uncovering illegal activities is absolutely impossible this way.**

Activity Log - Content

According to FB-I the access to 18 data categories should be possible through the “activity log”. In fact this tool does not live up to the promises of FB-I and even less to the DPA and Directive 95/46/EC.

The most obvious problem is, that massive amounts of data are simply missing in the “activity log”. Some categories like “pages visited” did not show up at all. Now they have even been totally removed from the “Activity Log”.

Other data seems to only show up on a random basis, with declining chances the further one goes back in time: For demonstration I have collected very obvious examples

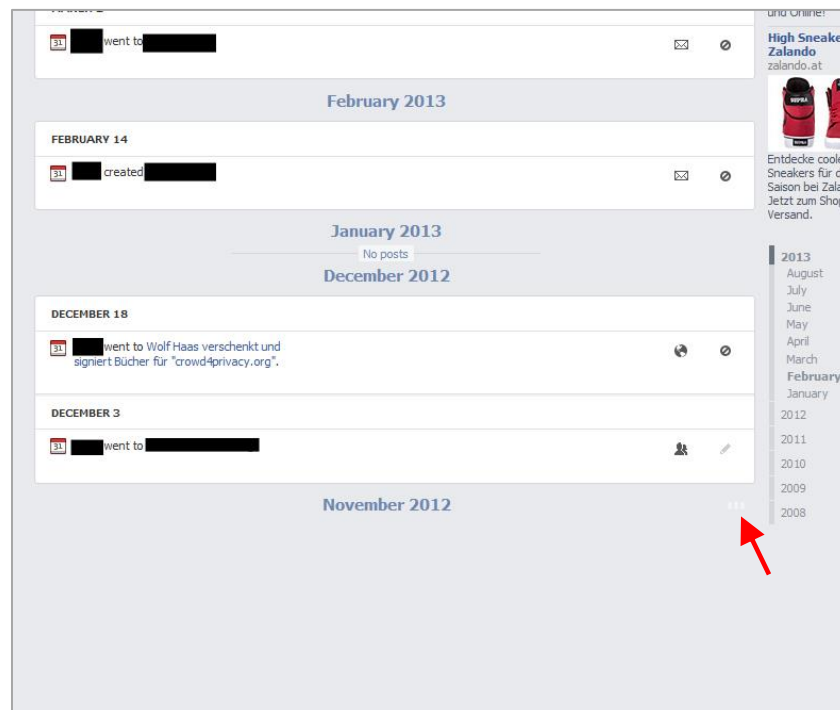


Screenshot: “activity log” for the years before 2010 (Taken in November 2012)

As a very obvious sign that the “activity log” was incomplete I experienced that the further one goes back in time, the less postings can be found. Interestingly there are certain dates shown, but no “activity” that would actually constitute the personal data. In the case of my account, there were only dates (and no activities or other personal data) for the time before 2010. The account is active since the June 8th 2008, so the initial 1,5 years (of about 4 years) were totally missing. This means that FB-I was not giving full access to the 18 data categories, despite claims that this data can be retrieved through the “activity log”. The data was held – as FB-I seems to have fixed this problem in the Summer of 2013.

➔ **F87: The 18 data categories in the “activity log” were not properly made available even 1,5 years after my initial “access request”.**

When doing further tests in August 2013 I also had to find that in many ways the “Activity Log” does still not work properly. Although I did not have the time to engage in strategic testing and I am not informed about the functioning of the tool it was often times not possible to load the “Activity Log” at all, especially when individual categories of data were selected. One example can be seen below. The “events” did not load despite reloading the page multiple times and clicking on all links available.



Screenshot: “activity log” does not load, “loading bars” blink for more than 10 Minutes.

➔ **F88: Despite the fact that there are less “bugs” the “activity log” is still suffering from obvious malfunctions and does not allow to access all data properly –2 years after my access requests.**

After I found the very obvious problems in November 2012, I have checked for more recent postings in the years after 2010. With a couple more clicks I soon discovered that also more recent data was simply missing. The first randomly picked comment was dated December 27th 2010 (so about one year after the total non-functioning of the “activity log”). When I scrolled to that data in the “activity log” there was not even a “lonely date” displayed. Reloading the page and clicking on “December 2010” or repeated scrolling (which makes the log load) did not change the result. In a similar way there were no entries for postings on other peoples’ walls, for videos and other data.

➔ **F89: There was no reference whatsoever to the comment on another users’ pictures, postings on other peoples pages or videos.**

The image consists of two screenshots of a Facebook interface from 2010. The top screenshot shows a post about a winter in Austria with a mountain photo and a comment from December 27, 2010. The bottom screenshot shows the Facebook Activity Log for December 2010, with a calendar on the right showing no results for the selected date.

Posting (27-12-2010)

All Categories 12-2010

NO RESULTS (!!!)



Even though the problem explained above was fixed in 2013, there are still postings on other pages that do not show up in the “activity log”.

For example the posting on the left from the Summer of 2008 was not properly displayed, since my “activity log” stopped in January 2009. There is a link for “2008” but the system does not react to clicking this link. There is also no reaction or symbol that would indicate that further data is loaded when one scrolls further to the bottom of the page.

→ **F90: Data from before 2009 is also missing in the “activity log”.**

Summary: “Activity Log”

In summary FB-I does still not deliver a solid data set through the “activity log”, this is more than two years after my initial access request which was filed with FB-I on June 2nd 2011. FB-I has had more than 20 times as long as the DPA allows FB-I to take to deliver a full, correct and all-embracing response to an access request, but still the result is simply not there.

- **F91: FB-I was allowed to take more than two years since the initial requests to develop and “fix” the “activity log”. The tool is however still not delivering the results it FB-I is claiming it to deliver.**
- **F92: Given the extensive time FB-I was given and the poor result, I have to conclude that the “activity log” is an obvious disaster.**

Other “Hiding Places” of Personal Data

According to the first report “Credit Cards”, “Linked Accounts” or “Payment Data” are again neither included in the various download tools nor the activity log, but in other placed all over facebook.com. This makes it again harder to for a user to get a full overview over what FB-I holds about them. Except from the credit card information (which is especially sensitive) this separation seems to have no other purpose than to hinder users to get a full overview of their data. This makes it obviously impossible for a normal user to just “get” his/her data. It is rather a treasure hunt for most users.

➔ ***F93: The two tools have to be subsidized by other “hiding” places to get a full(er) copy of data FB-I is holding. This is making it further impossible to get a clear picture about the processing of FB-I.***

Data not disclosed in any way

In addition to the not properly disclosed data in the various “tools” there is a whole realm of data that is obviously used by FB-I but not in any way included in any of them. While I hold a lengthy list of data that must be used by FB-I I hereby want to submit the following examples of data that is held by FB-I but in no way – and for no obvious reason – not included in any of the tools. This is – as previously – not an exhaustive list, but should only demonstrate there is much more that FB-I is not disclosing.

1. Changes in Fundamental Data (e.g. birthdate, name, password, change of the security question) are listed in the “download tool” however only the fact of a change is shown, not the factual change (old/new name, birth data or password). This data is clearly “personal data” and must be included.
2. Cookie Data is only shown by citing a couple of letters, but not the whole cookie code. There is no reason for this limitation.
3. The security question is not available to access.
4. ID Numbers of users, objects and postings are not included, despite being associated with a user or a users’ content and therefore constituting “personal data”.
5. Notifications (data from the notification box in the blue bar on top of facebook.com) is missing.
6. The category “Physical Token” from my PDF is missing.
7. The category “Realtime Activity” from my PDF is missing.
8. The data from “social plugings” is in no way disclosed. There is no evidence that such data is not held in a way that allows identification of a person – the policy is even saying that it does hold it in such a way for 90 days.
9. Deleted tags cannot be in any way seen or retrieved.
10. Deleted Groups, removed Event invitations and other such data cannot be retrieved.
11. FB-I is asking users if they “Know each other” in reality. This data is not shown anywhere.
12. In many cases FB-I allows to “undo” deletion. The data must therefore be held someway.
13. I have given my telephone number to FB-I as page admin which was even used to call me concerning placing advertisement on facebook.com. This number and other contract details are not disclosed.
14. On August 13th 2013 I have filled out a “survey” by FB-I, this data is not included.
15. Users can “unfollow” postings of others (e.g. if a user commented on a posting but does not want to get updated about this posting). This data is not included.

16. All data in relation to developers, page administration or advertisements is not included.
17. Page Invites (if others invite a user to a page) are not included.
18. Feed settings are only partly shown (it is e.g. not retrievable if users put in that they want more/less information from a person).
19. Chat Settings are not included (e.g. if you set that only some friends can/cannot write to you).
20. This information if a message/chat was done via a phone is not included (was in original PDF).
21. There is no information about the use of mobile phone “apps (e.g. ID numbers).
22. Users can choose not to see certain advertisement. This information is not retrievable.
23. When multiple people have a chat a person can “leave” the chat. This information is not in the download tool.
24. Other users can “suggest” to FB-I certain friends a data subject might know. This information is not shown.
25. FB-I is getting data from third party “data brokers” (see above – shadow profiles). This data is not included.
26. FB-I is re-targeting users through tracking technology. This data is not included.
27. If postings are “highlighted” or “hidden” this information does not show up in the “download tool”.
28. When something was “edited” by a user this is not displayed in the “download tool”.
29. The exact “meta data” (e.g. IPs, time stamps) are often times not shown, despite the fact that they have been in the original PDF.
30. Data other users have shared (e.g. through synchronization) and that is further used by FB-I.
31. Tracking of Page views on facebook.com (*“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”*)
32. Tracking Information through third parties (*“We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.”*)
33. Other information from third parties (*“Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.”*)
34. Often FB-I is showing questions (e.g. like the above mentioned “suggested hometown”). If a user has skipped or deleted it, this is not shown again. The fact that users have skipped such information must be retained in order to not show it again.
35. FB-I says it arranges postings according to the interest by users. This statistical data about a persons’ postings is not disclosed or shown (it is shown for “pages”).
36. FB-I is assessing how interested a user is in certain pages or other content. This has to be stored in one way or another to then generate a personalizes “news feed” or personalized suggestions in lists (e.g. when “tagging” a person, or when choosing a recipient of a message). In all these cases the lists are not alphabetical, but resemble the level or interest or interaction.

37. FB-I allows other users to “report” postings. This data is not disclosed to the reporter or the person that posted such content.
38. FB-I is using algorithms to e.g. automatically take down nude pictures. This function is not explained or disclosed.
39. FB-I is using algorithms to e.g. close accounts that it thinks are violating its policy. This function is not explained or disclosed.
40. FB-I is using algorithms to e.g. close or limit accounts that it thinks potential sex offenders. This function is not explained or disclosed.
41. FB-I is using algorithms to e.g. see what people are interested in. These functions are not explained or disclosed.

This is only a very rough list of things FB-I has or does and that data subjects are not supplied with. The DPC has to make clear what data FB-I is holding and what constitutes “personal data”, why it does/does not constitute “personal data” and if this data is properly and fully disclosed. Currently the DPC has only said that there is a list of very general “headlines”. All the rest is left in the dark.

➔ ***F94: There is a very long list of things that FB-I has to hold or produced in order to provide the service as it does today. This is not an exhaustive list, but just a demonstration that FB-I is clearly not making every bit of personal data available.***

➔ ***R42: I hereby request that the DPC***

- a) is establishing a list of all kinds of data FB-I is currently holding on its servers,***
- b) is confirming this list through cross checks with the servers operated in Sweden,***
- c) is confirming with FB-I the purposed of every such kind of data,***
- d) is assessing in a transparent way what data does and does not constitute “personal data”,***
- e) is informing me about its finding in an independently verifiable way and require FB-I to deliver all data in a tangible form before any decision in relation to my complaints is made.***

Purposes, Recipient and Sources

As I have pointed out previously, FB-I does not give data subjects relevant information in relation to the sources, recipients and purposes for each and every kind or bit of information. Currently FB-I sends out an automatic e-mail in response to access requests that simply refers to the privacy policy.

If data subjects want to know the specific purpose for a data category they will only find the following statement in the section ‘how we use the information’:

“We use the information we receive about you in connection with the services and features we provide to you and other users”.

WP 203 by the Article 29 Working Party:

The Article 29 Working Party has recently published WP 203 dealing with “purpose limitation”. In summary the Working Party has held that

“[t]he purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.” (WP 203, page 15)

The main issue seems to be that FB-I has to name the specific purpose for each processing operation. Currently FB-I is only referring to its privacy policy which is in no way meeting the requirements of the law concerning “shadow profiles” or “big data” analytics. As FB-I is using all data, from all sources for any purpose that relates to its business there is in essence no limitation whatsoever:

“We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”

The only thing FB-I’s wording does not allow is processing of data outside of the scope of its business and to share it with entities it does not have a relationship to. However as soon as FB-I is engaging in such activity it would be covered by the wording of FB-I’s policy. There is no way that a data subject can consequently know “*what kind of processing is and is not included within the specified purpose*”. As FB-I is factually allowing itself to use any data for any purpose FB-I does not “*allow that compliance with the law can be assessed*”. The Article 29 Working Party is even allowing for “layered notices” or “sub-purposes” for controllers, but FB-I has not reacted in any such way:

“It is generally possible to break a ‘purpose’ down into a number of sub-purposes.

- For example, processing an individual’s claim for a social benefit could be ‘broken down’ into verifying his or her identity, carrying out various eligibility checks, checking other benefit agencies’ records, etc.*
- The concept of an overall purpose, under whose umbrella a number of separate processing operations take place, can be useful. This concept can be used, for example, when providing a layered notice to the data subject. More general information can be provided in the first instance about the ‘overall purpose’, which can be complemented with further information. Breaking down the purposes is also necessary for the controller and those processing data on its behalf in order to apply the necessary data protection safeguards.” (WP 203, page 53)*

However FB-I has not even responded to “access requests” with a more “specific” purpose, but only referred to its privacy policy. Overall FB-I seems to perfectly fit into what the Article 29 Working Party was describing by this example:

“The above example can be contrasted with that of a large retail company selling goods via a website all across Europe and using complex analytics to inform personalised offers and targeted advertisements. In this case, the purposes must be specified in a much more detailed and comprehensive way, including, among other things, ‘the way in which’ personal data are processed. The decisional criteria used for customer profiling must also be disclosed.”

➔ **F95: The “specific”-test for the purpose FB-I is delivering is absolutely not met.**

The Working Party is further saying that data must be collected for an “explicit” purpose. When elaborating about this requirement the Working Party was finding that:

“The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. What is meant must be clear and should leave no doubt or difficulty in understanding.” (WP 20, page 17)

The wording by FB-I as outlined above can in no way meet this test. FB-I is using the vaguest wording possible when just talking about “others” and “other third parties” that they “may” collect data and only specify the purpose when saying the data is used “in connection with the service”. The very general statements are usually just accompanied by “examples” that do not limit FB-I in any way as they are just one case that falls under the general rule.

➔ **F96: The “explicit”-test for the purpose FB-I is delivering is absolutely not met.**

Summary – Self-Service Approach

Following what I have uncovered above it must be clear to everyone reading this section that FB-I does still not react to access requests adequately, despite the fact that they had more than two years, since the initial requests to respond to them. The tools are not functioning adequately and even if they would they would in no way be adequate to replace a “right to access” for data subjects.

FB-I makes it especially hard for users to access their data by spreading it out into different tools that are well hidden or take major effort to load, like the activity log. The data is currently spread out over different tools, pages and subpages. FB-I does not “deliver” the data, but lets the user go on a lengthy “treasure hunt” which is unlikely to be much of a great “evening entertainment” for most users. Instead this is clearly intending to distract users from getting all data. For inexperienced and average users it is currently impossible to download all data with reasonable efforts.

Many data fields that constitute “personal data” are missing in the various tools and pages that FB-I directs users to. Some data is simply not included (e.g. meta data or deleted messages), other data is “randomly” not accessible.

FB-I does not allow users to get a 1:1 copy of the raw data, but only gives users derivative data. This does not allow uncovering misconduct by FB-I, which is one of the ideas behind the right to access. I would have never been able to file the 22 complaints without access to raw data.

In addition FB-I is in no way giving proper information about the purpose(s) of every processing operation or every bit of data stored or used by it. The Article 29 WP was very explicit in its opinion on what is the minimal level of information that must be given. FB-I does in no way comply.

C. Non-User Access Requests

As a side topic I also want to mention FB-I's reaction to access requests by non-users. Currently FB-I allows to make an access request via e-mail through the address "datarequests@fb.com".

Even though this constituted a legally binding access request, FB-I responds with an automatic e-mail, talking about how users (not non-users) can access their data. In fact the only thing FB-I seems to do is sending a standard text back to whatever e-mail address was used to contact this e-mail.

As an alternative non-users can go to facebook.com (which makes them subject to FB-I's user tracking) and submit different information to an online form. After many reports I got from non-users I have filled out this form with various information from existing non-users and with false information. No matter what I did, there was always the same result: Even when I used e-mail addresses that have never existed, I got the information that FB-I holds "the e-mail address" and the "date where you were invited to join Facebook". This shows again, that FB-I is not taking access requests serious, is not even checking on the mere existence of the data it is holding about non-users.

➔ ***F97: In summary FB-I is not giving a material response to access requests by non-users, but "spams" data subjects with e-mails, independent from the individual situation of the user.***

This is another obvious breach of FB-I's obligation under the DPC and Directive 95/46/EC to respect the right to access by data subjects and shows FB-I's ignorance towards the rights of data subjects.

Summary – Access Requests

Facebook

In summary I could hardly believe the extremely dilettantish attempt by FB-I to comply with the right to access. After 2 years from the initial access requests FB-I has not been delivering a full, tangible, solid and somewhat valid response to my initial access requests. FB-I has not implemented a procedure that would possibly be compliant with section 10 DPA and Article 12 Directive 95/46/EC. It is obvious that FB-I was unable to demonstrate that I got all the data it is holding about me.

The wording of Directive 95/46/EC and the DPA are clearly indicating that the controller has to "deliver" the data and "supply" the data subject with the information after an initial access request. This wording clearly means an active ("push") delivery of the information. Users have no duty to go "treasure hunting" all over a webpage to get the data. Compared to a paper file this would equally mean that a controller has complied with the right to access by only giving a key to the files that are spread all over an archive. I would be able to accept if there is one file, that users can download and are directed to, but the right to access cannot be validly turned into a "right to hunt for data" without departing from the wording of the DPA and Directive 95/46/EC.

In addition I want to mention that I have never directly gotten any email or communication that would have invited me to use the new tools that were developed. The last email I got directly in relation to his initial complaint is an e-mail from 28th of October 2011, saying that all data was disclosed and that FB-I is not giving out further data.

ODPC

The ODPC has not only “waived” the legal deadline of 40 days for FB-I, but has also factually “waived” the duty to disclose the recipients, sources and purposes for the individual data categories. This is extremely problematic in relation to the rule of law and can in no way be upheld after the delivery of WP 203 by the Article 29 Working Party.

The ODPC has also managed to overlook the most basic problems in relation to the systems FB-I has deployed. This is raising serious questions about the ODPC’s technical and practical capability to analyze, investigate and research complex systems like facebook.com. While I am aware that the ODPC does not have the necessary personal and resources to investigate every line of code, I am stunned that it has not discovered the most obvious flaws of FB-I’s “self-service tools”. It only takes a couple of minutes of scrolling around and cross-checking to demonstrate that these tools are not functioning. If the ODPC was not able to discover such issues that are visible for every average user, it will be very hard to trust that more complex issues were investigated properly.

Without a copy of the raw data it would have been impossible to make the initial complaint. By not making FB-I produce a copy of the raw data the ODPC has massively limited my ability to make my case.

E. Amended Statement concerning Legal Consequences:

FB-I has not complied properly with my right to access under sections 4 to 6A DPA and Directive 95/46/EC (see all reasons stated above).

It has specifically not done so through sending the original PDF document. Much of the data now to be found in the different “tools” were not in any way included. FB-I has also not given such information within a 40 day period. It has not – until today – described the data, has not disclosed the purpose(s), the recipient or the sources. It has further not given me any subsequent information which would constitute a “notice in writing” or any other form of tangible information. It has not explained in an intelligible form data that is not understandable to me (e.g. “road block” in the download tool). It has also not given access to the logics involved in processing of such data.

➔ ***R43: I hereby – involuntarily - request that the DPC (after establishing the facts and delivering the relevant data as described at “R40” above) finds that FB-I has not complied with my right to access initially and as described here and in the initial complaint.***

➔ ***R44: In addition I hereby – involuntarily – request that the DPC finds that FB-I is continuing to not comply with the law. I ask the DPC to order FB-I to comply by sending me all personal data.***

14. Complaint 11 “Deleted Tags”

I ask the DPC to also consider the remarks made with complaint 03 “tagging” so that I do not have to repeat matters for this related complaint.

A. Facts described in the Original Complaint:

The Facebook Platform gives every user the possibility to “tag” other users or him/her. This is done by placing a box on the image that is shown in the picture around the face of the user in the picture. It is defined by coordinates that are saved with the picture (see data structure in attachment 03). The tagged or the tagging user can click a small link, called “remove tag” then the tag is not displayed anymore (see screenshot in attachment 04).

The Oxford Dictionary defines “to delete” as “to remove (data) from a computer's memory”, which clearly shows that by using “remove” the user expectation of “deleted” data is triggered. This is the same in many other languages that the Facebook platform is available in. For example, the German version uses the word “entfernen” which is the name of the “delete”-key on any German keyboard. The user experience is that the “tag” is gone and not displayed in any way anymore.

Surprisingly Facebook Ireland seems to only “deactivate” the tags but not delete them. This can be seen in the data structure that has a field called “active”, which indicates that there has to be an “inactive” mode as well (see attachment 03).

It can also be easily discovered by the fact that it is not possible to tag other users again in a picture where they have removed a tag (see attachment 05). This might be intended to protect the users, but in my opinion the only way of protecting the user when they are tagged is that they have to consent to the tag before it is saved on facebook.com.

In summary the user has the experience that the tag is deleted, while in fact Facebook Ireland is only deactivating the tag.

Since any purpose of the “tag” for the user and all possibility to process the “tag”-data is gone at the time the user clicked the “remove tag”-link, any further processing of the “tag” is done by Facebook Ireland, which must be seen as the sole controller.

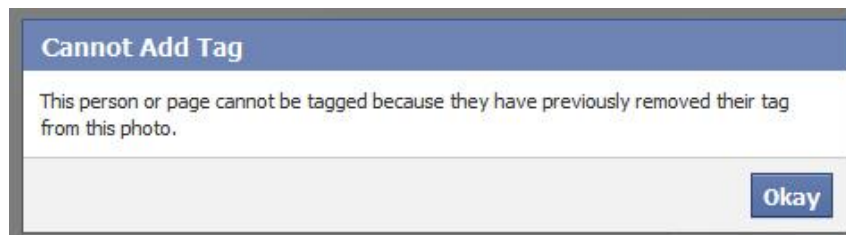
Under the section of Facebook Ireland’s privacy policy (see attachment 06) which describes the use of data by Facebook Ireland (“5. How We Use Your Information”), Facebook Ireland tells the user:

“We may use information about you that we collect from other Facebook users to supplement your profile (such as when you are tagged in a photo or mentioned in a status update). In such cases we generally give you the ability to remove the content (such as allowing you to remove a photo tag of you) or limit its visibility on your profile.”

The last sentence clearly states that photo tags can be “removed”, while the second possibility (limit its visibility) is only covering other “information”.

B. Reaction by FB-I and the DPC:

As outlined in the section on “Complaint 03 – Tags” I cannot see any major improvement, there seems to be no counterargument that I did not already anticipated in the initial complaint. FB-I is still not allowing users to remove information that was posted by others. There is also nothing in the reports that talk about FB-I’s usage of the data besides preventing re-invitations. This data may also be used for targeting ads, “friend suggestions” or other data processing by FB-I.



Screenshot: “Removed” tag is still kept to prevent users from “retagging”

The ODPC has stated the following in the “audit” documents in relation to “removed tags”:

“At present, the information provided to users in relation to what actually happens to deleted or removed content, such as friend requests received (not sent as what happens to those is the personal data of the recipient primarily), pokes, removed groups and tags, and deleted posts and messages could be improved. This is accepted by FB-I and this will be reflected in an updated Data Use Policy. From the control perspective, at present there is no facility for a user to delete (...) tags.

FB-I noted that it has already made changes to its service to improve visibility to users of data that previously was not visible. Facebook’s new profile, called “Timeline”, has a feature called “Activity Log,” on which many of the user’s actions around Facebook can now be viewed privately by the user. Since “Activity log” is only visible to the user, FB-I has proposed to use this feature as a means for users to access, review and delete their own data. (...) FB-I has also in this respect undertaken a policy of allowing users maximum control over their data and to the maximum extent possible will be extending an ability to delete on a per item basis individual data items.”

“FB-I’s response on these complaints highlighted that it retained such information for what it termed various important purposes to provide the best possible experience to users. For example, it stated (...) FB-I uses removed tags to prevent the user from being re tagged in the photo.”

- ➔ **F98: FB-I has in no way changed the way it processed “removed” tags. There is no way for a user to really delete such “tags” that are placed by other users.**
- ➔ **F99: FB-I expressly says that it uses such deleted tags for “various important purposes”. There seems to be no justification for such use under any circumstances.**

C. Legal Consequences described in the Original Complaint:

1. *There is no transparent notice that these bits of data are still held. In contrast to that the user is told that the poke is “removed”, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*
2. *There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. In contrast to that it even tells the user that the “tags” get “removed”. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.*
3. *There is no longer a legitimate purpose for holding on to these bits of data. There is no other purpose for these bits of data specified by Facebook Ireland. The data would have to be deleted according to section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
4. *The further processing of these bits of data is no longer relevant for the purpose of the processing and seems to be also excessive, which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
5. *The processing of the data seems to be longer than necessary to fulfill the purpose and therefore seems to be illegitimate. This would constitute a breach of section 2(1)(c)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*
6. *It seems that there has never been an informed consent, by the user to the use of these bits of data, since the user just agreed to the processing with having the option to “remove” this content later. If Facebook Ireland does not remove any of this content, the consent seems to be not informed and not unambiguous and therefore void under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*

D. Additional Statement on the Legal Consequences:

7. *FB-I confessed to use the data for “various other purposes”. This is a clear violation of the principle of “purpose based processing” and therefore a violation of Section 2(1)(c)(ii) DPA and Article 6(b) of Directive 95/46/EC.*
- ➔ ***R45: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

15. Complaint 12 “Data Security”

A. Facts described in the Original Complaint:

Facebook Ireland holds excessive amounts of highly personal information. This includes personal messages, relationships, comments, a list of interests, religious and political beliefs, location information or visited events (including events that e.g. indicate political, religious or sexual preferences). Depending on the political system a user is living in and on the specific content of the information, this bears tremendous security risks for the user. The mere fact that a user is or was “friends” with a person, has interacted with a person, or has been invited to an event (such as demonstrations) might be very risky for the individual user. But even the mere masses of “normal” information that is saved on Facebook Ireland’s servers makes attacks by hackers, identity thieves or secret services very likely. It seems to be only a matter of time until someone finds a way to access Facebook Ireland’s data, just like it has happened to many other companies before.

A) Encryption

Despite these facts, according to its privacy policy, Facebook Ireland only seems to be encrypting passwords and credit card numbers (see attachment 03). This is questionable, since all other private information would not even be encrypted when a security breach would occur.

B) Statements

In addition to that, Facebook Ireland gives the following statements in its terms and privacy policy:

1. *“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.”*
2. *“We do our best to keep Facebook safe, but we cannot guarantee it.”*
3. *“WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES (...) WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE.”*
4. *“FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.”*
5. *“WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS (\$100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS.”*

These statements 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) Applications and “Skimming”

Facebook Ireland is allowing and promoting third party “applications”. These applications allow third parties, which might not even fall under the European privacy system, or any equivalent scheme (such as the Safe Harbor Agreement). There are some general provisions that developers of applications have to follow, but even the most basic provisions (such as providing some kind of privacy policy) are not consequently enforced by Facebook Ireland. Since every user can grant an application access to all information his/her friends are sharing with him/her, these applications bare a tremendous risk for data security. I could not think of another data controller that gives third parties such a broad and uncontrolled access to personal data.

A lot of information is automatically shared with “everyone” on the internet, some information has the be shared with “everyone”. This bares a high risk of “skimming”. An example would be the project of two artists that imported the faces and names of millions of Facebook Ireland’s users for “lovelyfaces.com”.

B. Reaction by FB-I and the DPC:

FB-I was granting wide access to user data

As outlined in the initial complaint, the complaint is mainly based on the provisions of FB-I’s terms. In this relation I have the feeling that the ODPC’s investigation has revealed what I have suspected. The first report has made clear that FB-I was not following laws, which is shown by these statements:

“We were somewhat concerned that the provisioning tools in place for ensuring that staff were authorized to only access user data on a strictly necessary basis were not as role specific as we would have wished to see.” or “Many policies and procedures that are in operation are not formally documented. The absence of these documented policies and procedures means that it is difficult to assess the audit trail data stored by Facebook within the context of their information security policy.”

➔ **F100: From the findings in the report I am satisfied that the complaint was justified as FB-I did not have proper restrictions in place.**

Technical Analysis

While I could generally understand the findings of the “technical analysis” in the report and I also feel that they are generally supporting the facts and views I have submitted I was wondering which exact methodology the ODPC and the external expert have deployed in respect to FB-I’s security measures. Some statements in the report only relied on submissions by FB-I but did not independently verify compliance:

“The majority of the controls described by Facebook appear to be effective.”

➔ **F101: The “audit” seems to have in no way tested or reviewed the proper functioning or even the existence of these controls. It also just says that “the majority” “appear” to be effective.**

Some statements in the report seem to suggest, that just by the fact that breaches were not all over the media, there is no reason to doubt or investigate into actual compliance:

"If large-scale, frequent data breaches were taking place on Facebook's corporate networks, it is believed 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."

→ **F102: According to this logic every atomic power plant is "safe", as long as it has not turned into another Chernobyl - a claim that can be made, but does not seem to be very helpful.**

C. Additional Submission of Facts:

The rational of the "external expert" and the ODPC is especially questionable if we look at hackers, data dealers and other criminal (or illegal) activity. These people are usually working in secret and will not broadcast their hacks on the BBC. FB-I (or its parent) has recently started a campaign to pay hackers that were able to access their systems (see CNN.com). It would e.g. be more relevant to have FB-I disclose the awards and reports that FB-I got through this campaign, in order to get a solid understanding of how well FB-I is sticking to its obligations under the law, than just looking at the media.

In this relation I also want to mention that it was possible for "Open Data City", a German company for data visualization to "scrap" the friend lists of more than 200 profiles, which were friends with me. The information was used to generate e.g. the graphic that can be seen above at "Complaint 02 – Shadow Profiles". This demonstrates that it is possible to scrap substantial data if only individual users are targeted (e.g. by private investigators). Other cases (with wider media coverage, see e.g. [this American report on YouTube](http://this.American.report.on.YouTube)) was e.g. "lovely-faces.com" which was mentioned in the initial complaint. In this case artists were able to scrap about one million profile pictures of FB-I's users.

Another wonderful example is "profileengine.com" that has scrapped millions of profiles from facebook.com, including profiles that were set to be "private" and not to be open to search engines. The website claims to be a "public social network" and that the DPC of New Zealand has approved of it, because the relevant information was "public" when scraped (see profileengine.com/help).

There are profiles of different members of our group, like this profile on me: [profileengine.com/#/people/\[redacted\]](http://profileengine.com/#/people/[redacted]) Profiles of other members of our group show even more data publicly (see e.g. [profileengine.com/#/people/\[redacted\]](http://profileengine.com/#/people/[redacted])).

When I was searching the web for news, I soon found many other stories about scrapping and other forms of security breaches on facebook.com:

- Very recently FB-I has e.g. disclosed the telephone numbers and email of 6 Million users. (<http://www.reuters.com/article/2013/06/21/net-us-facebook-security-idUSBRE95K18Y20130621>)

- Repeatedly hackers managed to access the profile of Mark Zuckerberg.
(<http://www.buzzfeed.com/gavon/mark-zuckerbergs-hacked-facebook-photos>)
(http://money.cnn.com/2011/01/26/technology/facebook_hacked/index.htm)
(<http://www.telegraph.co.uk/.../Mark-Zuckerberg-Facebook-profile-page-hacked.html>)
- Even the first “audit” report names another incident where pictures were accessible (see page 109).

So overall we look at everything but a “clean record” when looking at FB-I’s data security history. The “audit” has in no way changed this picture as it seems to have only relied on hearsay. It seems more than questionable if “FTR Solutions” (which is factually just a home office) was in any way able to professionally assess the technical, administrative and factual data security of an incredibly complex and huge system like “facebook.com”.

- ➔ ***F103: There have been a number of high profile “hacks” into Facebook and recently even data breaches directly caused by FB-I. There was no proper limitation of access within the company on a “need to know” basis.***
- ➔ ***F104: The “audit” has not established any verifiable facts concerning this matter. It has merely relied on hearsay and absurd arguments (“not reported”).***

D. Legal Consequences described in the Original Complaint:

The facts listed above and the statements of Facebook Ireland make it more than questionable if Facebook Ireland is really securing the user’s data in a way that is sufficient under section 2(1)(d) and section 2C DPA and Article 16 and 17 of Directive 95/46/EC. This seems to be especially questionable if you look at the mere amount of information, the possible sensitivity of it and the rather easy access to the stored information.

- ➔ ***R46: I hereby – involuntarily - request that the DPC is establishing reliable facts and finds that FB-I was unable to demonstrate in a verifiable way that it is having proper protection mechanisms in place, based on the frequent scandals FB-I is engaged in. I ask the DPC to order FB-I to take the necessary steps.***

16. Complaint 13 “Applications”

A. Facts described in the Original Complaint:

Facebook Ireland offers all its users the option to use third party “applications” on facebook.com. These applications are developed, managed and run by third party companies that can be situated anywhere in the world. The applications run on external systems but Facebook Ireland allows the providers of the applications access to the data it is hosting. According to Facebook Ireland’s statistics page there are more than 20 million applications installed by users every day.

This constitutes a tremendous threat to data privacy on facebook.com. There are only very limited contractual measures that Facebook Ireland is taking to ensure that developers of applications have an adequate level of data protection (see the yellow text in attachment 03).

There is no way that Facebook Ireland would be able to ensure real compliance with these limited contractual measures. The Wall Street Journal found out in October 2010 that “all of the 10 most popular apps on Facebook were transmitting users’ IDs to outside companies” (see attachment 04).

Another example: Many applications do not even have a privacy policy, even though Facebook Ireland requires this. When I was checking on the 12 applications Facebook was randomly suggesting on my profile, 4 did not have a policy while 5 did have a policy right after I clicked on them (see attachment 05). Apparently Facebook Ireland is not even enforcing this very basic provision.

When the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy (see e.g. page 5 of attachment 05).

While Facebook USA is a member of the Safe Harbor Agreement, developers are not obliged to be a member of Safe Harbor. This means that Facebook Ireland is exporting personal data to other companies that do not have an adequate level of data protection, including companies in the USA which are not member of the Safe Harbor.

Most users are not aware that if a “friend” on facebook.com installs an application, the application can automatically access their profile picture, name and other basic information (see privacy policy in attachment 06). Note that Facebook Ireland is hiding this consent for the use of other users’ data under the section “my basic information” (see e.g. page 4 in attachment 05)

If the person that is installing the application is consenting to it, the application can read all information about all friends that the person can see. Again this means that not the data subject but “friends” of the data subject are consenting to the use of personal data. Since an average facebook user has 130 friends, it is very likely that only one of the user’s friends is installing some kind of spam- or phishing application and is consenting to the use of all data of the data subject. There are many applications that do not need to access the users’ friends personal data (e.g. games, quizzes, apps that only post things on the user’s page) but Facebook Ireland does not offer a more limited level of access than “all the basic information of all friends”.

All this can only be prevented if the user turns off “platform” (opt-out). This can be done by clicking a button which is again well hidden (see attachment 07). There is no possibility to use applications without the possibility that other users can access the user’s data (all or nothing). The data subject is not given an unambiguous consent to the processing of personal data by applications (no opt-in).

Even if a data subject is aware of this entire process, the data subject cannot foresee which application of which developer will be using which personal data in the future. Any form of consent can therefore never be specific.

Facebook Ireland could not answer me which applications have accessed my personal data and which of my friends have allowed them to do so. Therefore there is practically no way how I could ever find out if a developer of an application has misused data it got from Facebook Ireland in some way.

B. Reaction by FB-I and the DPC:

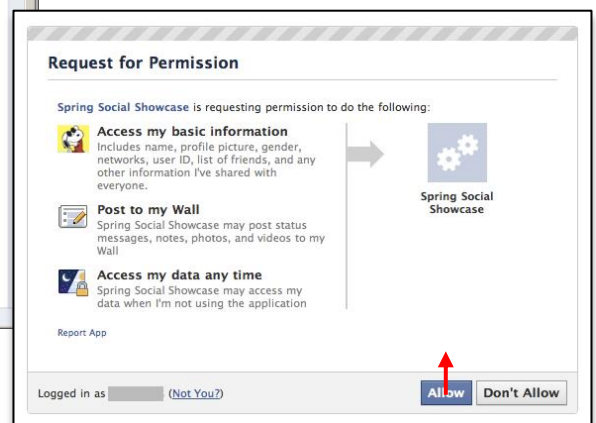
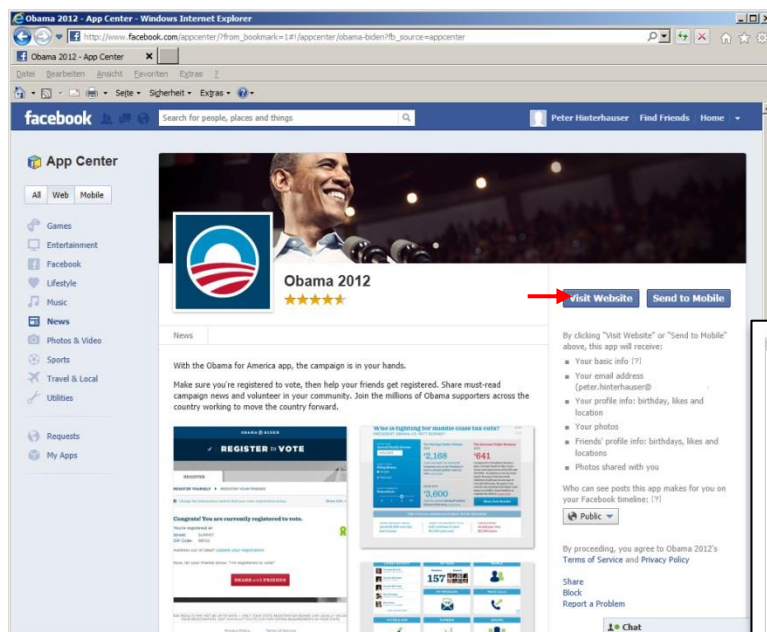
Changes

I welcome the thorough investigation by the ODPC into third party apps, I especially thought that the insight on the possibility to “trade” tokens to be very interesting and problematic. I want to highlight that, despite the rather clear language on the side of the ODPC, there were no material changes by FB-I. The only step that seems to have derived from my initial complaints seem to be that FB-I wants to deploy a system that checks if there is a life link to a privacy policy, but this still seems to be developed from what I could read in the review. I also welcome the possibility to select the audience for posting by an app that the ODPC has pushed for.

On the other hand I had to observe that FB-I has taken a big step back in user information and getting a clear, informed and unambiguous consent when changing to its new “app center”. While I thought that the previous system made it rather clear that “something happens”, the new system is a step backwards to a system that does not make it clear that the users’ data is now transferred out of facebook.com and that this might be critical. I doubt that all users understand this procedure und the new setting. While the old system (see below) was titled “Request for Permission” and was clearly indicating that the user

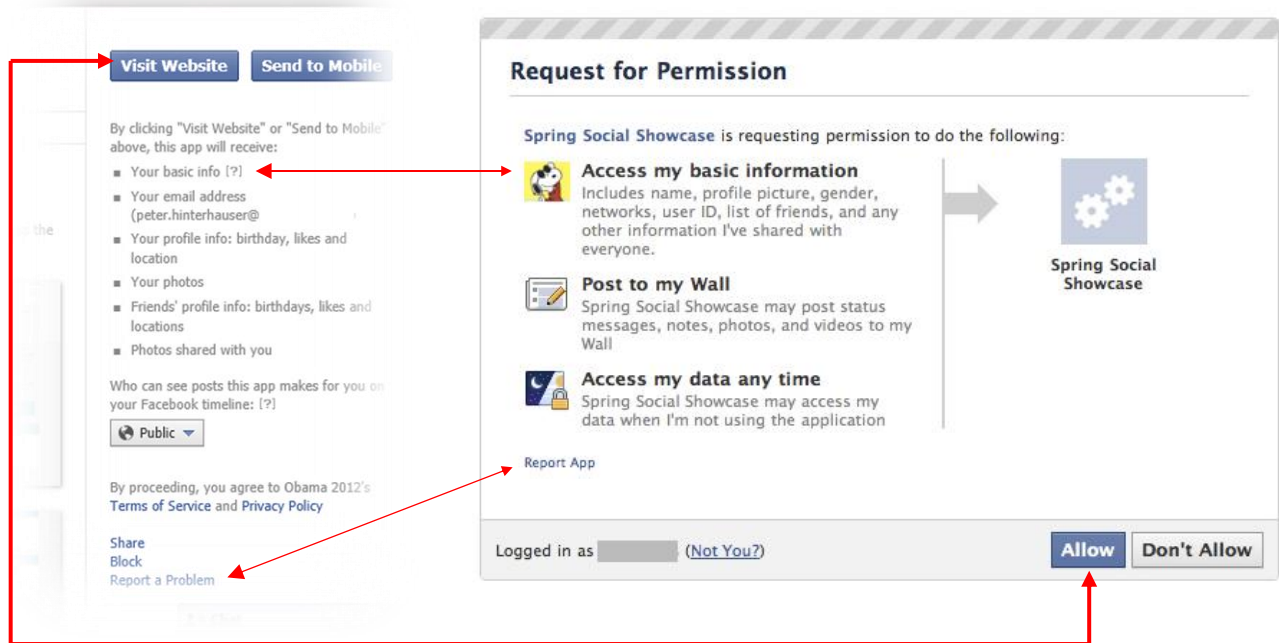
grants something by using buttons labeled “Allow” and “Don’t Allow”, the new version does not use such wording.

In the example on the left, there is no headline and the button is simply called “Visit Website” and is not indicating to grant anything.



Screenshots: New System (Left), Old System (Right)

If these two versions are looked at a little closer and “side-by-side” it is easy to see that the essence of the agreement was moved into subtext or totally deleted. As an example “basic info” was describes as also including the whole friends list of a user, while this can now only be seen if a user “hovers” over the little question mark. The information on what other allowances cover was totally removed. The text was changed from a *black, bold and central information* to a *small, grey text on the side* (comparison below).



Screenshots: New System (Left), Old System (Right)

Overall this is clearly a step back: The new system reminds me of the old “sign up” process (see complaint 08) before FB-I improved this process. I have e.g. already seen a headline like “your basic info” as fraudulent when this also includes friends’ data, but when this information is now even hidden behind a tiny grey question mark, I have no reason to think that the initial complaint is not even more justified.

➔ **F105: FB-I has taken a huge step back when changing the “app” sign up process. There is no unambiguous consent anymore. All the other problems are however still remaining.**

“Consent by Third Parties”

The main issue I brought up was the problem that users can forward personal data of all their friends to an external application, without any notice or even consent of the data subject. FB-I has simply claimed in this respect during our talks in Vienna that the other users consented for the data subject.

This would be a legal miracle, since making legal arrangements without getting the power by the subject of these arrangements is impossible ever since the Roman law. Unless FB-I would be able to underpin this miracle with solid arguments I am currently not willing to accept this explanation.

Another approach that FB-I might take is claiming that by consenting to the policy and not turning off the “platform” option (again: this is an opt-out that users are not actively informed about) this would constitute consent. The problem is, however, that the user would be blankly consenting to a form of processing of any controller for any purpose and under any policy. Such a form of consent is under no way legally binding and would never be in line with the law that requires an *informed, specific and unambiguous* consent.

→ ***F106: There is no way that FB-I gets valid consent from a third party to forward personal data to a third party, without any knowledge or information of the data subject.***

Arrangement with Third Parties

It is a core principle of Directive 95/46/EC that data must be contained in a legal sphere where the right to data protection is factually enforceable. As the ODPC has rightfully outlined in the report it is insufficient for FB-I to claim that by posting some terms on their page this would factually ensure compliance. To further develop this problem I also want to point to the content of these requirements do not fully ensure compliance with European law. The privacy policies of applications are often not even remotely defining the basics. In addition, an “app developer” can stay totally anonymous by using a fake account. FB-I can currently only “turn off” such apps, but has no way to prevent developers from uploading new apps or even pursuing breaches of the law.

While users might be able to consent to having their own data transferred out of a solid legal sphere (if they are controllers of their page/timeline) this is unacceptable for third party data. Only where developers are identified, are situated in an “adequate” country or are bound by an agreement that ensures factual legal consequences when breached, FB-I could possibly allow access to third party data.

In addition facebook.com is full of fraudulent, misleading or “spam” application that are exactly using these loopholes to access users’ data and conduct in illegal behavior. FB-I is facilitating this.

→ ***F107: FB-I is not ensuring that data is held within a sphere of providers that are ensuring an “adequate” protection of the data subjects’ right to data protection.***

C. Legal Consequences described in the Original Complaint:

1. *There has never been an informed specific and unambiguous consent, by the data subject to the use of personal data. All processing of third party data is therefore illegitimate under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EC.*
 2. *There is only limited information in Facebook Ireland's privacy policy. The consent to the use of friend's information is hidden under the section "my basic information". Accurate information is needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes a breach of the principle of fairness in Section 2(1)(a) of the DPA.*
 3. *There seems to be a breach of the principle of purpose-based processing. The user shares personal data for the use on facebook.com but not for another purpose of some third party "application". This breaches section 2(1)(c)(i) DPA and Article 6(1)(a) of Directive 95/46/EC.*
 4. *The possibility of developers to access personal and potentially sensitive data without any prior checking by Facebook Ireland and very limited enforcement of the most basic provisions cannot be seen as processing with appropriate security measures as necessary under section 2(1)(d) DPA and Article 17 of Directive 95/46/EC.*
 5. *Facebook Ireland does not ensure in any way that the developers of applications ensure an adequate level of protection for the privacy and fundamental rights and freedoms of the data subjects as necessary under section 11 DPA and Article 25 of Directive 95/46/EC. Consent of the data subjects to the transfer is unlikely since many applications do not have a policy that would explain to which county the data is flowing and the actual data subject is not even asked.*
- ➔ ***R47: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

17. Complaint 14 “Removed Friends”

A. Facts described in the Original Complaint:

Facebook Ireland gives its users the possibility to “add” and “unfriend” other users as “friends”.

Surprisingly, Facebook Ireland does not delete “unfriended” users totally but saves specific information about “removed friends” such as time, date of the removal and the user that “unfriended” the other user (see attachment 03). After using Facebook for 3 years, Facebook Ireland already lists 13 (!) pages of removed friends for my account.

The data subject does not suspect in any way that these former friendships are still saved and not fully deleted. The user experience is that the former friend is “gone”. It is questionable if users are always comfortable that former relationships are still held by Facebook Ireland. For example, it might not be in the interest of the user that government agencies or other subjects can find out that a certain relationship has existed before. The user “adds” friends with the knowledge that they can “unfriend” them at any time and therefore removes this information at her/his own liking, this raises the question if a user is really giving an informed consent if the option to delete a relationship is in fact not available.

Facebook Ireland might use this information for its “friend” suggestions but it seems that the sole purpose of Facebook not suggesting “removed” friends later on is disproportionate, especially if we suspect that at some later point these friends might want to contact each other again.

B. Reaction by FB-I and the DPC and Additional Facts:

The reports did not exactly deal with the complaint and the substance of it. FB-I has indicated in the first report and also in our direct talks in Vienna, that “deleted friends” are only used to prevent these users to be suggested to the person again. Removed friends can at the same time send another invitation any time. Only when users have additionally “blocked” the person this is not possible.

In the first “audit” report from December 2011 FB-I is cited with the following explanation:

“... FB-I uses removed friends data to ensure that the removed friend isn’t surfaced as a friend suggestion to the user; ...”

While this small “benefit” of not suggesting removed users to be added again, this purpose does not seem to be proportionate to keeping all deleted friends for an indefinite time. It also would not really harm any user if previous friends show up once in a while. (In fact FB-I constantly shows people in the “people you might know” section that users mainly do not want to be friends with, otherwise they would be added.)

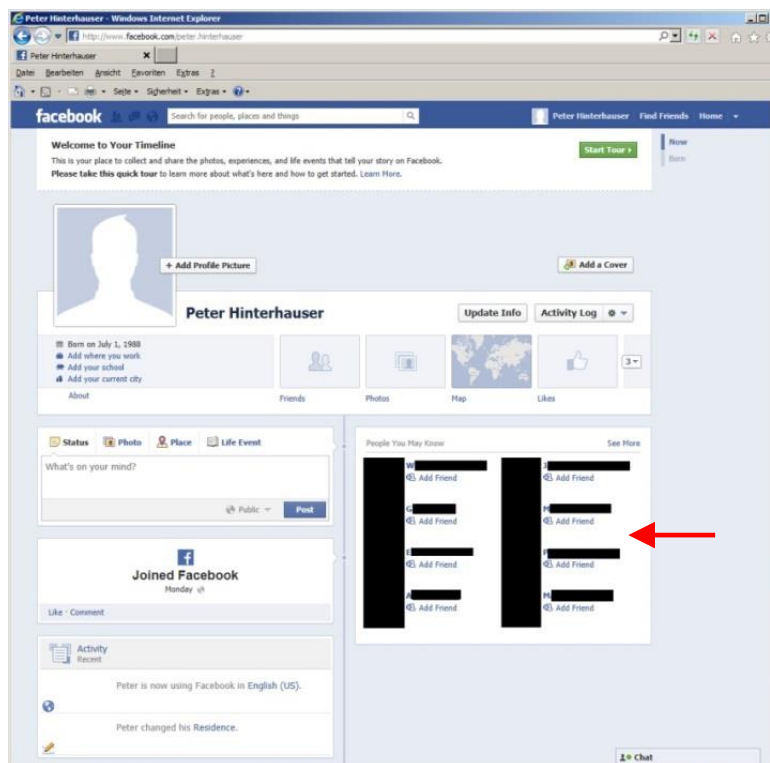
➔ **F108: It is not proportionate to hold all deleted friendships just for a little better “suggestions”.**

Further Use of “Removed Friends”

Independent from this question of law, I also found a new phenomenon that plays into the original complaint and FB-I’s reaction to it. While FB-I claimed in the report and in our talks in Vienna that it was only using the “deleted friends” to not suggest the same person again, I found that FB-I was in fact processing this information further to suggest the friends of the deleted friend to a person.

To show this I have opened a new profile. This profile was friends with my real profile. Both profiles were used to be able to make some screenshots. After this the friendship was “unfriended”. Following the “unfriending” FB-I was still suggesting (only) my friends to the test profile.

In a further step I have additionally deleted everything that in any way related to my “real” profile in the “Activity Log” of the test profile. My “real” profile did also not display or show anything that would in any way relate to the “friendship” with my test profile. However even after a considerable time FB-I has continuously suggested the friends of my “real” profile to my “test profile”.



Screenshot: Deleted friends used to promote “people you may know”

This case also shows that despite FB-I and the DPC finding that data is “deleted” one can often times find ways to show that FB-I is in fact still holding such data. This means that FB-I has given false and misleading evidence or at least not said the truth when asked about such processing operations.

- ➔ **F108: FB-I has made false statements to the ODPC about the use of “deleted” friends. FB-I uses “deleted” for other purposes than just not suggesting deleted friends.**
- ➔ **F109: This is another case that lowers the credibility of FB-I’s**

C. Legal Consequences described in the Original Complaint:

1. *There is no transparent notice that this personal data is still held. In contrast to that, the user is told that the friend is removed, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
2. *There is no information in Facebook Ireland's privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) of the DPA.*
3. *There is no longer a legitimate purpose for holding on to this personal data. There is no other purpose specified by Facebook Ireland. The data would have to be deleted according to section 2(1)(i) DPA and Article 6(1)(b) of the Directive 95/46/EC.*
4. *The further processing of this personal data is no longer relevant for the purpose of the processing, which constitutes a breach of 2(1)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
5. *The processing of former friends becomes excessive if you think that Facebook Ireland does not have a final date of deleting the information. If all former friendships get saved for an indefinite time, this clearly is excessive as defined in section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*
6. *The processing of the data seems to be longer than necessary to fulfill the purpose and therefore seems to be no longer necessary. This would constitute a breach of section 2(1)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*
7. *It seems that there has never been an informed consent by the user to the use of this personal data since the user only agreed to the processing including having the option to remove this information later. If Facebook Ireland does not remove any of this content, the consent seems to be not informed and not unambiguous and therefore void under Section 2A(1)a DPA and Article 7(a) of Directive 95/46/EC.*

D. Additional Statement on the Legal Consequences:

In addition to the original claims I want to mention that the fact that FB-I is using "deleted" friends for other purposes than previously said is additionally a breach of the laws cited above (see 1, 2, 5, 6). In addition the "further processing" is clearly non-compliant with the previously specified purpose:

8. The "further processing" of this data does not seem to be "compatible" with the initial purpose in most cases which constitutes a breach of 2(1)(c)(ii) DPA and Article 6(1)(c) of Directive 95/46/EC.

➔ ***R48: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

18. Complaint 15 “Excessive Processing of Data”

A. Facts described in the Original Complaint:

Facebook Ireland is gathering excessive amounts of personal data of an unbelievable mass of people worldwide. It is very likely that no government or cooperation has ever managed to gather such a huge amount of personal (and often highly sensible) data.

After using facebook.com for 3 years, Facebook Ireland gathered more than 1.200 pages of personal information about me (in fact Facebook Ireland might hold a much bigger amount of data, see Complaint 10), even though I have deleted just about everything I could (e.g. all my posts, all messages, and many friends) See a compressed version of the PDF as attachment 03. If Facebook Ireland goes on like this for another couple of years, it will have gathered even more personal data about even more people.

All this information is not only hosted by Facebook Ireland (in its role as a processor) but it is also continuously processed in the company’s role as controller (see attachment 02). Facebook Ireland is using this information in order to show advertisements and suggest friends or aggregate information on its “news feed”.

If this practice continues, the masses of data will clearly be excessive for the limited purpose of the secondary use of Facebook Ireland (as indicated in attachment 02).

I doubt that Facebook Ireland really needs access to all data it is hosting in order to conduct its own purposes. In fact, information that is only a couple of days old will not show up in news feeds, after a while Facebook Ireland’s “friend suggestions” will have been shown 10 times without response and a page a user visited one year ago will not be relevant for today’s advertisements.

Another aspect that justifies the limitation of excessive processing of data is the question of data security (see also complaint 12). The central processing of private data of more than 700 million users bears significant risks for data security. Data that the user processes on Facebook Ireland’s servers might never be 100% safe, which makes raises the question if all the data is really necessary in the first place. It is undisputed that the best form of data security is data minimization.

Considering all these arguments I think that Facebook Ireland’s processing of all hosted data for its own purposes is a prime example of excessive processing of personal data and therefore illegitimate under section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.

B. Reaction by FB-I and the DPC:

The two reports did not analyze the claim in my complaint, but only remotely touched on it. There is only one excerpt from the counterargument by FB-I that made it into the first report:

“FB-I, inter alia, pointed to the worldwide popularity of the platform and contended that the fact that Facebook processes the data of a very large number of people does not in itself mean that that processing is excessive. Furthermore, FB-I noted that processing is excessive where it was unnecessary, not simply where it justifiably involved a large amount of personal data.” (First Report, Page72)

C. Additional Statement on the Reactions:

This statement misses the point. The initial complaint has never said that the fact that FB-I runs a popular service is by itself excessive. The second argument, that only “unnecessary” processing of personal data would be “excessive”, is totally ignoring the wording of Section 2(1)(c)(iii) DPA and Article 6 of Directive 95/46/EC. The fact that processing must be “necessary” in relation to the purpose is already enshrined in Section 2(1)(c)(i) since it has to be obtained for one purpose, data that is not necessary is by definition not allowed to be processed. The additional rule that it should also not be “excessive” in relation to the purpose means that the data processing should (even when within the purpose) not be disproportionate.

Often times a purpose can be served in many different ways. As long as every step of the process is necessary to get a certain result, it is generally within the principles of the law. But at the same time the same purpose might be able to be served through less intensive, narrower, leaner processing.

In other cases there is simply a disproportion by the large, intense and broad processing of endless amount of personal data for a purpose. As an example FB-I might be able to predict even better what users are interested in by having 100 times the amount of information it already has. It might be even better with 1 Million times the amount of data. It might become even better when cross referencing this with the same amounts of other people and so on... All this processing is “necessary” if you want to deliver perfect results, but at some point it is “excessive” given the purpose of selling a couple more ads.

If FB-I holds thousands of pages of data and uses all this information for any operation of FB-I, partners, developers and so on. I believe that the level of limitless processing is reaching a level that is “excessive”. Given the practically limitless purpose, the endless options to cross reference data, the massive amounts of data that FB-I is getting and generating about users and the fact that much of this data is not directly visible (see complaint 02), I have to ask the DPC: If this form of “big data” is not excessive, what is?

As outlined in the initial complaint FB-I would need to limit the data that is available for a specific purpose (e.g. only use certain data – meaning certain types or timespans) and FB-I has to enable users to “recycle” old junk data by allowing for mass deletion (this was e.g. introduced by FB-I for the “search history” in the activity log, but not for any other type of data). The same though was also used by the ODPC when discussion about advertisement (report, page 41) - in the end this is about proportionality.

➔ ***F110: FB-I has not brought forward any meaningful argument. The element of “excessive” processing is independent from others and well defined in any data protection law book.***

D. Legal Consequences described in the Original Complaint:

Considering all these arguments I think that Facebook Ireland's processing of all hosted data for its own purposes is a prime example of excessive processing of personal data and therefore illegitimate under section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.

I therefore kindly ask you to take the necessary steps to change this illegal practice by Facebook Ireland.

I think there can be many practicable solutions to this problem. Two solutions which might need to be combined to make the processing by Facebook Ireland non-excessive would be the following:

- a) The user needs to get reasonable options to delete old data that he/she does not need anymore (e.g. a setting that deletes old postings, comments and other data after a couple of weeks automatically – "digital forgetting")*
- b) There has to be a limitation on the use by Facebook Ireland of the user's old data.
Google for example deletes old IP-addresses after 9 months, even though they might not even constitute "personal" data and they are not necessarily subject to European law.
On facebook.com this could e.g. be done by "archiving" them, which would mean that Facebook Ireland would not be allowed to use them anymore and is only "hosting" them.*

- ➔ R49: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.**
- ➔ R50: If the DPC finds this form of processing not "excessive" then I am hereby asking the DPC what it would consider "excessive"?**

19. Complaint 16 “Opt-Out”

A. Facts described in the Original Complaint:

Facebook Ireland is frequently claiming in public statements that the users consented to the use of their data. This would be within the legal boundaries of the Irish and European regulations. In fact Facebook Ireland is generally following an opt-out-system:

1) No Consent

When signing up to facebook.com the users are consenting to a privacy policy but not to specific settings, since none of the documents specifically lists the settings. The users could have just consented to a general framework but did not consent to any specific setting. This means that there is a lack of specific consent in the first place (see privacy policy, attachment 03).

The consent is also not unambiguous since the user never clicks on a check-box or anything that could be seen as an unambiguous act (see David Kelleher, in Privacy and Data Protection Law in Ireland, Page 210).

2) Collection of Data before the possibility to change settings

When the Facebook user goes through the standard process as it is designed by Facebook Ireland, the user gives the following information during the “first steps” (see attachment 04)

- 1. Importing all e-mail-addresses of other data subjects from his e-mail-provider*
- 2. Information about his education and employee*
- 3. His picture*

When the user proceeds through this process, he is then asked to give the following additional information (see attachment 05):

- 4. More profile information*
- 5. Activate his mobile phone*
- 6. Type in more friends*

As the very last point (that is not even shown on the start screen, if now scrolled down) he will find a link to an information page about privacy on facebook.com (not the page for the settings!)

This means that according to the sign-up process of Facebook Ireland, the user is publishing his/her information before he will ever have the possibility to change any of the settings. The privacy settings are not even a part of the sign-up process. This is especially worrying since Facebook Ireland’s privacy policy and terms are tying many consequences to these settings like e.g. limitations on deleting the data, sharing the data or IP rights.

3) Standard Settings

The standard privacy settings are very liberal. Most settings are set in a way that anyone on the internet can see the content and even search engines can index all the content. Even very sensible information such as “religious views” are set to “friends of friends” (see attachment 06). Since an average user of

facebook.com has 130 “friends” this means that this sensible information is viewable to about 16.900 “friends of friends”.

That these privacy settings are more in the interest of Facebook Ireland than the users’ can be seen if one looks at statistics about the preferred privacy settings. From my personal experience most users set their settings to more private ones than originally set by Facebook Ireland, despite the discouragement by the barriers on facebook.com.

That these settings are too liberal can also be seen if we look at the legal obligations of the user of facebook.com. Following the “Lindquist” decision (06.11.2003, C-101/01) and the Article-29 Working party paper 5/2009, the user falls under the DPA him-/herself if he processes third party information that is visible to more than just his friends. This would be even true for his “friend list” or maybe pictures of third parties that he posts on his facebook page. The standard settings that Facebook Ireland uses are far off this Irish and European understanding of privacy and are instead following a rather US-American understanding of privacy. Facebook Ireland also does not inform about the legal obligations of the user that follow the standard settings.

4) Barriers and discouragement when opting-out

For inexperienced or older users it is very hard to change all settings.

Generally Facebook Ireland “hides” many settings. On the main page there are a couple of big buttons that are accompanied by very small links (see attachment 07). Many settings can only be seen when the user clicks on these small links. E. g. these important settings cannot be edited on the main page:

- Editing the access of third party applications to the users’ information*
- Editing if search engines can find the user’s profile (can be found under “apps and websites”!)*
- Editing the face recognition system of facebook.com*
- Editing who can “tag” the user in pictures, videos or other elements*
- Editing who can publish the current location of the user*

Facebook Ireland has claimed in the past that these main settings should make it easier to find the most important settings (see e.g. here: <https://www.facebook.com/blog.php?post=391922327130>) but in fact all the important settings above are now “hidden” behind small links. The user has to find settings at absurd places (such as the option to be found on public search engines under “apps and websites”).

Even after the user has clicked on these links, there is the general rule that the more invasive the use of data is and the more the user wants to restrict it, the more clicks he/she has to make.

For example, sharing information with a smaller group than “friends” (e.g. only certain groups of friends, or not sharing them at all, “only me”) is not suggested, but takes another click on “custom settings”. Certain settings are not even shown at all on the main menu, but the user has to click on “edit settings” in order to see the settings in a new window and change them (see attachment 08).

The user is generally discouraged by Facebook Ireland to change the settings rather than informed on what the functions mean. For example, when the user wants to change the settings that control which data applications of other users can access, there is no option to “unselect all” - the user has to remove

18 (!) check marks individually. The prompt is accompanied by the following statement: “The more info you share, the more social the experience” (see attachment 09).

In many windows Facebook Ireland shows that other friends are using a function too but of course they do not show the friends that opted out (see attachment 10). This tells the user not only that other friends use it too but indicates that the user should act just like them.

B. Reaction by FB-I and the DPC:

Sign-Up Process

The first part of the complaint addressed the sign up process. This has been changed in a way that was surely a step in the right direction (see also Complaint 08 above) – especially the problem that users had to enter data without any knowledge of the policy and the settings seem to be solved.

➔ **F111: FB-I has changed the sign-up process towards a system that is closer to the law. I therefore see my original complaint to be justified in this respect.**

Standard Settings

On the other hand FB-I still uses the most privacy-unfriendly settings as default settings, there seems to be no change whatsoever during the last year. This is not in line with WP187 and WP163. The reports do not explain how FB-I’s “best practice” approach can be contrary to very clear and the most basic recommendations by the Article 29 Working Party that it has published exactly in relation to default settings of social networking sites:

“(…) Because of the uncertainty as to whether the lack of action is meant to signify consent, not clicking may not be considered unambiguous consent.” (WP187, Page 24)

The ODPC also took the view in the first report that the current approach by FB-I was not satisfactory and that there must be a meaningful change to the current opt-out approach:

“This Office has no difficulty with FB-I expressing its position as to what it believes a person should select to gain the greatest experience from the site but we do not accept that the current approach is reflecting the appropriate balance for Facebook users. By extension it is clearly the case that the process also needs to be adjusted for current users to take account of this approach. This Office therefore recommends that FB-I undertake a thorough re-evaluation of the process by which it empowers its users both new and current to make meaningful choices about how they control the use of their personal information.”
(First Report, December 2011, page 40)

Other than the new “information” (four pages and 104 words) that is presented to new users, there seems to be absolutely no change by FB-I (see more details above at Complaints 08).

➔ **F112: FB-I has not changed its “Opt Out” policy - despite the very clear recommendation by the ODPC and a very clear interpretation of Directive 95/46/EC through WP187 and WP163 that make an “opt-out” system clearly necessary.**

Usability / Deterring Users

The reports did not cover the claim that FB-I deters users from choosing more privacy friendly settings, other than citing a counterclaim by FB-I that does not deliver any material arguments. It is still a long and tiring work to go through countless pages, subpages, pop-ups and deactivate one check box after the other, which leads in fact to users just giving up on it.

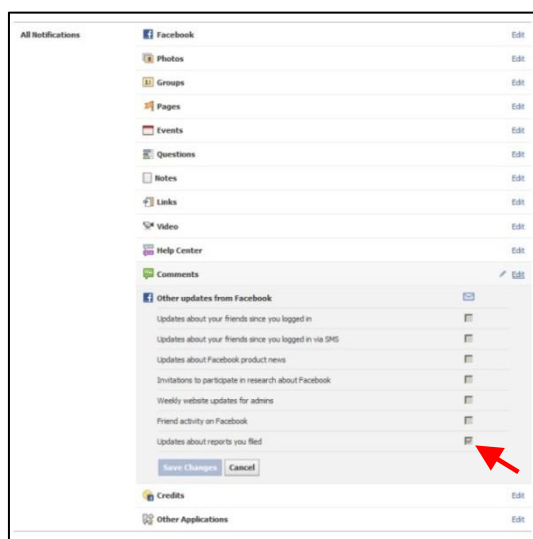
The report has also asked FB-I for settings on an “per item basis”. This already exists on most pages, but turns out not to be very privacy friendly. Users can only change individual settings or delete individual items of information. When users e.g. do not want applications to get any data and express this wish thorough the form above, they have to uncheck 17 (!) check boxes (picture on the next page).

Currently it is also factually impossible to delete all old “post”, old “messages” or participation in old “events”. By making it technically impossible for users to express their wishes in a common form, FB-I ensures that it is harvesting more and more data, without any realistic chance of users to mitigate this. I suspect that this is planned in a “big data” strategy (see above, complaint 02 “Shaddow Profile”). Any other provider of cloud services (e.g. web mail, video pages or online office software) allows for mass deletion or mass manipulation of the users’ data - everyone, but Facebook.

➔ **F113: FB-I is making it unduly difficult to delete or “opt-out” from the use of data, by making deletion impossible, offering no general settings and only allowing “per item” deletion.**

FB-I’s “Auto Opt-In”

In fact FB-I has even departed further from the legal requirement to offer “Opt-In” function by “adding” checked boxes for users whenever FB-I changes something about its system. When users have gone through the trouble of unchecking all the boxes, FB-I simply added new boxes that were again checked, instead of respecting the clear wish of the users that has unchecked all boxes.



Screenshot: FB-I “added” the users’ consent & 17 (!) Check-Boxes

This is not only problematic in relation to the “unambiguous consent” by the data subject, but there is no way that this could be seen as a form of “fair” processing of users’ data. Instead of some action or even inaction FB-I is simply “ticking the boxes” as it wished, even after a user has made its settings.

➔ ***F114: FB-I has even departed further from the goal of an “unambiguous” consent, by not only “adding” new boxes, but also “adding” the users’ consent, even if users have clearly indicated their wishes by unchecking every single box.***

C. Legal Consequences described in the Original Complaint:

I think that this practice of Facebook Ireland is illegal under the following provisions of the DPA and Directive 95/46/EC:

- 1. There is no specific, informed and unambiguous consent by the actual data subject (opt-in). This constitutes a breach of section 2A DPA and Article 7(a) of Directive 95/46/EC. In contrast, to seek the unambiguous and informed consent of the user, Facebook Ireland is discouraging any change of preset settings (opt-out). This makes any processing by Facebook Ireland generally illegitimate.*
- 2. The information is not obtained fairly because the user is only getting one-sided information and is generally discouraged by Facebook Ireland to change the privacy settings. This breaches section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*

I therefore kindly ask you to take the necessary steps to change this illegal practice by Facebook Ireland. In my understanding the privacy options have to be “opt-in” in a way that the privacy settings are set to the highest level of privacy, or at least to a level that makes the processing by the user legitimate under section 3B(4)(c) DPA and Article 3 of Directive 95/46/EC. This would be given when all settings are set to “friends only”. The settings should be part of the sign-up process that new users go through and could be accompanied by neutral information. I think under these conditions the use by Facebook Ireland would be legitimate. Existing users would have to go through such a process again since there is no valid consent of these users at this time.

➔ ***R49: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

➔ ***R50: If the DPC is departing from the very clear interpretation by the Article 29 Working Party I hereby ask the DPC to explain why he does so.***

20. Complaint 17 “Like Button”

A. Facts described in the Original Complaint:

Facebook Ireland provides scripts that providers of webpages across the web can implement in their webpages. Facebook Ireland refers to them as “social plug-ins”. The most common one is the “Like” button, which enables the user to click on it and therefore share the webpage it is placed on with all his “friends” on facebook.com.

Besides this basic functionality the “like” buttons are also used by Facebook Ireland to track the users across the web (see investigation of the DPC of German Schleswig-Holstein). Most webpages now have “like” buttons which enables Facebook Ireland to track users not only on some pages but on the major part of their internet activities.

This is even more worrying if we consider that “like” buttons can not only be found on “normal” pages such as news, company or entertainment sites, but also on pages that contain sensitive information (e.g. pages of political parties, action groups, churches, porn sites, websites containing health information or pages of trade unions; see attachment 03). The user does usually not know if the website has a “like” button before visiting it and can therefore not make informed and specific choices.

Facebook Ireland changed its underlying system for the “like” button previously from a more privacy friendly version to the current version. The old version (called “sharer”) still works but cannot be found in Facebook Ireland’s online documentation and is not promoted anymore. The key difference is that with the old system, the “like” button was only a link to a page on facebook.com. When the user clicked a button on a webpage, a pop-up opened and the facebook.com page was shown to the user (see e.g. the “share” link on www.europe-v-facebook.org). There was no interaction with Facebook Ireland if the user did not click on the link. Now Facebook Ireland only provides a more sophisticated version of the same button that shows the number of people that already liked the website. This button results in an interaction with Facebook Ireland in the very moment the page is first visited.

Facebook Ireland’s privacy policy does not directly say what information Facebook Ireland Ltd. gets when a user visits a page with a “like” button. In the section “About social plugins” Facebook Ireland says “We receive data when you visit a site with a social plugin. We keep this data for 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people’s data in a way that it is no longer associated with you.”

The information that Facebook Ireland gathers every time any user is visiting a site is the following: date, time, URL, and “other technical information” including the IP address, browser information and operation system information (see attachment 04). In addition to this the DPC of German Schleswig-Holstein found out in a technical study that Facebook Ireland also reads cookies that Facebook Ireland has placed in the users’ browser cache. This cookie is placed when a user interacted with facebook.com, including users that did not sign up to facebook.com but only visited it facebook.com, or visited some person’s or company’s public page on facebook.com. The cookie stores an individual ID that allows tracking

individual users over longer periods of time (cookie is valid for 2 years). A user has the possibility to delete cookies, but users of facebook.com are also traced by IP addresses that usually are the same for every user over a certain period of time.

Facebook Ireland claims that the data is only used for “improving its systems”. It seems questionable what exactly the improvement is in this case. Facebook Ireland does not answer how the collection of random users that did not even interact with a social plugin on some external site is in any way useful for “improving” facebook.com. For whatever reason, Facebook Ireland replaces individual IP addresses of German users, as Richard Allen, a spokesperson of Facebook Ireland Ltd told the press in Schleswig-Holstein. Users of other European countries like Ireland or Austria are tacked with their individual IP address.

If this practice is compared to the telecommunications data retention directive (Directive 2006/24/EC) it seems very problematic, that a private company is, without any obligation to do so and without any specific purpose, logging detailed information about the webpages a user visited. Facebook Ireland Ltd. is not only logging the IP addresses of users, but also knows their names and can connect all website visits to an extended pool of other information. The data is not held on European territory, but in the US and Facebook Ireland does not guarantee any sufficient forms of data security, as telecommunication providers under the Directive 2006/24/EC are required to. There is no guarantee that US law enforcement agencies or European authorities do not access this sensitive information of European citizens. No matter if Facebook Ireland is using the collected data for illegitimate purposes the mere fact that these (unnecessary) data are held is a tremendous privacy risk that seems to be out of proportion.

B. Reaction by FB-I and the DPC:

The reports have dealt excessively with social plugins and I welcome the steps in the right direction that derived from it (like e.g. FB-I’s pledge to delete the last bit of the IP addressed).

On a factual level the reports and the technical analysis did not deliver any substantial new outcomes. The information that is transferred between a users’ computer and FB-I when social plugins are loaded was already discovered before my initial complaints. I also believed that the website, that uses social plugins through an iframe, does not get direct access to the users’ data. There has not been further information about what data constitutes (potential) personal data and what does not.

- ➔ ***F115: FB-I does not contest that it does generate personal data about users that visit websites off facebook.com when they load (not interact) a social plugin. This information is stored for 90 days.***
- ➔ ***R51: It has yet to be checked if also non-users (of users with separate browsers) can be tracked in a personal way (e.g. by connecting the browser cookie with a person). I ask the DPC to investigate on this or disclose all information that would clarify this question.***

Purpose

After repeatedly reading all documents from the ODPC I can only see that FB-I has claimed

“that it has not designed its systems to track users and non-users browsing activity”
(first report, page 82).

Version 1: In FB-I’s submission from July 2012 they say that “The Report Audit has confirmed that (a) FB-I did not use the data it received when logged-in users visited sites with social plugins for advertising purposes, and (b) FB-I only used such data for the purposes of bug-fixing and analysis of social plugin performance.”

Version 2: During our talks in Vienna, FB-I said that the data is used to (a) find bugs, (b) check on the success of a like button and (c) to generate statistics for the page owner. The last purpose (statistics for web pages) cannot be found in the documents of the audit. Therefore I have to assume that the audit failed to list all purposes FB-I uses the data for.

Version 3: In addition to the purposed listed above the “security” argument was also deployed in a letter sent to me by Richard Allen, which would constitute another purpose not listed in the two reports.

Version 4: In its policy FB-I does have special provisions concerning the purpose of social plugin data. The section on social plugins does in no way limit the use of such data, instead it is covered by the core provision for all data it receives, which says that

“We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”

➔ **F116: FB-I has deployed at least 4 (!) versions for which purposed the data is used for, which is again raising questions about the credibility of FB-I’s claims. Under its policy FB-I may use such data for any purpose.**

Technical Report

The technical analysis shows an attempt to look into the “black box” by randomly clicking pages. This attempt could have delivered compelling results, which it did not. But just by the absence of obvious relations between webpages that where visited and ads, I cannot conclude that the data is not used in any other or more complex way. Targeting systems are very complex and might not deliver obvious results after browsing different pages for a couple of minutes or even an hour. This was also concluded in the report, which only says that such obvious relations could not be found, but does not say that their non-existence is a fact.

In this relation I also want to draw the attention to the first and second test on page 184 of the first report: There was no reaction by the system no matter if users have just loaded or interacted with like buttons in relation to “parenting/childcare”, while there was a relation in later tests concerning “motor-bikes”, “Harley Davidson” and “Cisco”. If there would be a 1:1 relation, such difference should not occur.

The technical report also says that all accounts were brand new and did not have friends. FB-I has pointed out repeatedly that there might be multiple factors (e.g. posting something and liking something else) that triggers the advertisement system. Only browsing pages would surely be considered a weak indicator of users' interests compared to "likes" of products and postings about certain topics.

→ ***F117: While the technical report has ensured that there is no blankly obvious connection between "social plugins" and advertisement it was unable to ensure that there is generally no such link. It did not cover any other correlations (e.g. security, statistics, newsfeed composition).***

Overall I have to conclude that there are indications for the exact purpose, but no solid evidence for what exact purposes FB-I uses the "social plugin" data exactly. The purposes named in the reports do not match up with the purposes I was given by FB-I.

→ ***F118: There is so far no evidence that FB-I only uses such information to "fix bugs", "analysis of social plugin performance". In our talks it was e.g. also claimed to be used to "generate statistics for the page owner" or for "security purposes". Therefore the reports are clearly incomplete.***

Consent

FB-I says that it has consent for the generation of such data through the privacy policy. The question at stake is not if there could be some act of consent to a policy that explains this behavior, but if this consent can be "informed" and "specific":

A user cannot predict which pages have a "social plugin" before loading the page. The core of a *specific* consent is, that a data subject cannot give blanket consent to any operation. Data subjects will usually feel very different about tracking on a news page, political page, one concerning health, sexual orientation, religion or a porn page (I have submitted examples of such use in the initial complaint).

When FB-I says that by signing up to facebook.com data subjects have allowed it to track users anywhere on the web, no matter of the content, time and purpose, FB-I ignores that consent must be *informed* and *specific*. This is not the case and there is currently no counterargument by FB-I. This is in essence also the view that was shared by other DPCs in Europe, like the German "ULD".

The reports and documents also do not take into account the other reasons I have submitted in the initial complaint that make the form of processing illegitimate. I especially want to stress that it does not elaborate more privacy friendly approaches (e.g. the "two click" solution) that would constitute a more privacy friendly alternative that has to be taken to fulfill Section 2(1)(c)(iii) DPA.

→ ***F119: The DPC and FB-I have in no way explained how a user may have consented to such processing. It has also not covered any of the other issues brought up in the original complaint.***

C. Legal Consequences described in the Original Complaint:

1. *There is no specific, informed and unambiguous consent by the actual data subject. This constitutes a breach of section 2A DPA and Article 7(a) of Directive 95/46/EC. The data subject is tracked no matter if it is a user of facebook.com or not and without any specific prior notice.*
 2. *The information is not obtained fairly because the user does not have sufficient information from the privacy policy and their data is obtained before the data subject has any chance to see if the individual webpage uses a “like” button. This breaches section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*
 3. *The purpose of the “like” button is to share a URL or other information with friends on facebook.com. Facebook Ireland is using this functionality to also establish an intensive tracking scheme across the web by further processing the information. This constitutes a breach of section 2(1)(c)(ii) DPA and Article 6(1)(b) of Directive 95/46/EC.*
 4. *The collection and retention for at least 90 days of all the data listed above for the mere purpose of transferring the URL of the “liked” page is inadequate, irrelevant and excessive and therefore breaches section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*
 5. *The older version of the “like” button shows that there are ways of providing the same service in a more privacy friendly way. This means that by providing it with today’s specifications breaches section 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC.*
- ➔ **R52: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.**
- ➔ **R53: If the DPC is departing from the very clear interpretation by the Article 29 Working Party on consent and purpose limitation I hereby ask the DPC to explain why he does so.**

21. Complaint 18 “Obligations as a Processor”

A. Original Complaint:

As explained on the previous page, Facebook Ireland is a “cloud service”. This means that users have the possibility to store data on Facebook Ireland’s systems of which they are the data subject. Users are also able to process information of third parties.

Following the Irish DPA and the Directive 95/46/EC Facebook Ireland is a classic “processor” whenever the data concerns a third party, while the user is the actual controller. This means that all users within the European Union have to comply with Article 17 of Directive 95/46/EC.

As an example for one national law the Irish DPA reads:

Section 2C

(...)

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall—

(a) ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the data controller and the data processor and that the contract provides that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with obligations equivalent to those imposed on the data controller by section 2(1)(d) of this Act,

(b) ensure that the data processor provides sufficient guarantees in respect of the technical security measures, and organisational measures, governing the processing, and

(c) take reasonable steps to ensure compliance with those measures.

When the different functions of facebook.com are observed and the terms of Facebook Ireland are read it seems clear that a user of Facebook Ireland’s services has no contractual guarantees that have to be given according to the Directive 95/46/EC and the various national laws within the EU.

Instructions. All data about a third party that a controller (user) is uploading is initially included into the system following the controller’s (user’s) instructions (e.g. by clicking a button). From that point on Facebook Ireland is processing all data for various unclear purposes and there is very limited control or even instructions of the data controller. The controller (user) usually only instructs Facebook Ireland to simply host the information.

The controller (user) usually does not instruct Facebook Ireland to analyze hosted third party data for the purpose of advertisement, friend suggestions, the aggregation of news feeds or whatever other purpose Facebook Ireland processes data for (the specific purposes of processing are unclear, see complaints 08 and 10).

In other cases it seems obvious that Facebook Ireland is not even following the instructions of the controller (user) as can be seen in different complaints I filed concerning “removed data” that was still stored by Facebook Ireland.

Obligations & Security Measures. *Facebook Ireland is explicitly not guaranteeing any technical or organizational security of hosted personal data (see complaint 12). This means that under the current terms Facebook Ireland and all controllers (users) within the European Union are breaching the relevant national data protection laws whenever they process any third party data on facebook.com.*

Compliance. *Facebook Ireland has no system that allows the user to ensure compliance with the obligations Facebook Ireland has. The obligations may be different in each member state of the EU and would make it necessary to have a very transparent and open system that each controller could access. There is no such system on facebook.com, there are only individual help pages and links the controller can follow but there is in no way a clear management system as controllers of e.g. webhosts, blogs or video websites are employing. Under the current privacy regime it seems also impossible to develop such a system because there is no clear rule on who is the controller, processor or data subject of a particular piece of information.*

I think Facebook Ireland and all its users can only process data legally on facebook.com if:

- Facebook Ireland clearly defined who are the controllers and who is the processor of each piece of data,*
- Facebook Ireland does not process third party data that controllers upload for any other purpose as hosting (or other processes the controller is fully in control of) and*
- Facebook Ireland gives the controller the possibility to ensure compliance with its obligations.*

B. Reaction by FB-I and the DPC:

Please refer to the section “General Remark: Controller” above that also covers this complaint. The reports have not made any essential remark in relation to the problem I have pointed out. There is also no statement from FB-I that I could find in the reports. In general statements FB-I is flip-flopping on this matter as it pleases. The ODPC has also not taken a stringent standpoint throughout the “audit”.

→ F120: As outlined above FB-I and the DPC have not taken a position on this crucial question. However there are clear indications towards the system I have originals submitted as this seems to be the only system that would allow operating facebook.com under EU laws.

C. Legal Consequences:

I generally refer to the original complaint. If FB-I is mixing up its role as processor and/or controller it is not only violating section 2C but also about every paragraph of section 2(1) and (2) DPA as well as Articles 16, 17(3) of Directive 95/46/EC and just about every part of Articles 6 and 7. I am awaiting more detailed information from the DPC and FB-I to assist with further clarification, depending on the exact roles FB-I is claiming to have as well as the position the DPC is taking.

- ➔ ***R54: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***
- ➔ ***R55: In addition I am requesting that the DPC is making a clear assessment of the different roles of FB-I, Facebook Inc, the users and others (e.g. application developers) and base the all other complaints on such an assessment.***

22. Complaint 19 “Picture Privacy Settings”

A. Facts described in the Original Complaint:

Facebook Ireland Ltd. gives all users the possibility to upload pictures that are then hosted on facebook.com and also processed by Facebook Ireland Ltd. for its own purposes. All users are given the option to choose specific “privacy setting”. The options are “public”, “friends of friends”, “friends only” and “only me”, as well as customized lists of users.

Facebook Ireland is heavily promoting these options and makes users believe that only the chosen circle of people can access the pictures that were uploaded (see attachment 03).

After reading the source code of the picture pages of facebook.com we easily found out that all URLs of pictures started with “http://fbcdn-sphotos-a.akamaihd.net/hphotos-ak” and were followed by numbers, of which a part was the (public) UserID of the Facebook user. The URL is registered with “Akamai Technologies Inc.” situated at 8 Cambridge Center, Cambridge, MA 02142, USA (see attachment 04). This means that Facebook Ireland Ltd. has outsourced the delivery of the content to “Akamai Technologies” as a “Content Delivery Network”. From a legal standpoint this company is a processor that is bound by privacy laws. All actions of “Akamai Technologies” are undertaken on behalf of Facebook Ireland Ltd.

To our surprise, the picture were accessible at the URL despite privacy settings that should prevent this from happening. This means that anyone that was ever able to see the URL has potential access to the pictures.

After little research online we could also find guides on how to find (embarrassing) pictures that people have removed or hidden from a specific user on facebook.com (see attachment 05).

This means that Facebook Ireland is not really having a proper access management system but is only “hiding” links to pictures that are public on the internet. The URL mostly consists of consecutive numbers and the (public) UserID. Only the last couple of numbers seem to be random numbers that may protect the content against “brute force” attacks (see a list of URLs in attachment 06). Even the most basic webserver have a system that does not only “hide” links but actually limits the access to the content itself.

In a recent update Facebook also promoted the “new privacy settings” that include the option to change privacy settings after posting a piece of information (see attachment 03):

Change Your Mind After You Post?

Before: Once you posted a status update, you couldn't change who could see it.

Going Forward: Now you'll be able to change who can see any post after the fact. If you accidentally posted something to the wrong group, or changed your mind, you can adjust it with the inline control at any time.”

In fact only the link is hidden from the users, but not the content. Users that have accessed the picture before can find the link in the cache of a web browser and still access the link directly.

It seems very likely that Facebook Ireland's systems for other content (e.g. videos) follow the same general rules so that I would encourage the DPC to investigate all other forms of content delivery by a third party as well.

B. Reaction by FB-I and the DPC:

The report and the technical analysis did not bring forward any new facts or arguments that were not already known in the initial complaints. My guess that one part of the URL functions as a key against attacks was verified and seems to be effective against external attacks, but this was not the point.

The reports did not elaborate about the legal questions that were brought forward in my complaint. Most notably the question whether it is adequate to allow users to only control the “password” (being the URL) to the picture, while telling the users that they can control the audience of the picture itself.

FB-I's security concept works like a hotel room that is opened via a code. The code is not changed when new guests arrive, allowing former guests to get into their former rooms. This problem was not touched.

→ F121: The DPC and FB-I have not reacted to the key point of the complaint. This is that the “password” is handed out to anyone once able to see the picture. While the user has the impression he can control the availability of actual file he can in fact only control the availability of the link to the file. If a third party revived the link he cannot take it back.

C. Legal Consequences described in the Original Complaint:

1. *There is no transparent notice that users can only control the links, not the actual content. The user is told that only a certain group of people can “access” the data while in fact anyone can access it. This breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
2. *There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) DPA.*
3. *It seems that there has never been an informed consent to this form of processing, since the user just agreed to the processing by having the option limit the access at any given time. If Facebook Ireland does not really limit the access to the content but only the access to the link, the consent seems to be neither informed nor unambiguous and therefore void under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EC.*

I therefore kindly ask you to take the necessary steps to change this illegal practice by Facebook Ireland and make Facebook Ireland comply with Irish and European law. I think that this could only be achieved if Facebook Ireland sets up contractual and technical measures to ensure that the content delivery networks limit the access in the very moment that the settings are changed on facebook.com.

D. Additional Statement on the Legal Consequences:

In addition I want to also make the following claim, since FB-I is being the processor/controller of such data it must also ensure proper security of data held under the law. This seems to be another violation of the law:

4. *FB-I is either violating section 2(1)(d) DPA if the DPC is understanding that FB-I is the controller of such data, or it is violating section 2(1) DPA if the DPC is of the opinion that FB-I is acting as processor in respect to these pictures. This means that FB-I is correspondingly violating Article 16 and/or Article 17 of Directive 95/46/EC.*

The whole problem could easily avoided if FB-I would just hand out a new “code” segment for the picture as soon as the settings are changed and is also deleting the original picture under the previous link.

➔ R56: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.

23. Complaint 20 “Deleted Pictures”

A. Facts described in the Original Complaint:

Facebook Ireland Ltd. gives all users the possibility to upload pictures that are then hosted on facebook.com and also processed by Facebook Ireland Ltd. for its own purposes. All users are given the option to delete their hosted pictures whenever they want to do so. After clicking on “delete” the user is asked: “Are you sure you want to delete this photo?” After the user agrees by clicking “confirm”, the picture is not shown to the user anymore.

Facebook’s Privacy Policy reads:

“When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).”

After reading the source code of the picture pages of facebook.com we easily found out that all URLs of pictures started with “http://fbcdn-sphotos-a.akamaihd.net/hphotos-ak” and were followed by numbers, of which a part was the (public) UserID of the Facebook user. The URL is registered with “Akamai Technologies Inc.” situated at 8 Cambridge Center, Cambridge, MA 02142, USA (see attachment 03). This means that Facebook Ireland Ltd. has outsourced the delivery of the content to “Akamai Technologies” as a “Content Delivery Network”. From the legal standpoint this company is a processor that is bound by privacy laws. All actions of “Akamai Technologies” are undertaken on behalf of Facebook Ireland Ltd.

To our surprise, the deleted picture was accessible at the URL after we deleted it from facebook.com. After a couple of minutes we tried loading the pictures again and it was still available. Even 32 hours later the deleted picture was still available on the servers of “Akamai Technologies” (see attachment 04). The next time I checked was the next day in the afternoon (about 48h from deletion), where the picture was finally not available anymore.

This means that anyone that was ever able to see the URL has potential access to the deleted files. After little research online we could also find guides on how to find (embarrassing) pictures that friends deleted from facebook.com (see attachment 05).

As a data controller or processor Facebook Ireland Ltd. can only outsource to a (sub-)processor if it can guarantee that the company is guaranteeing full compliance with the obligations set down in section 2C(3) DPA. In addition to that we were unable to find “Akamai Technologies” on the Safe Harbor List (see attachment 06).

It seems very likely that Facebook Irelands systems for other content (e.g. videos) follow the same general rules so that I would encourage the DPC to investigate all other forms of content delivery by a third party as well.

I also encourage the DPC to investigate if “Akamai Technologies Inc.” has some form of agreement with Facebook Ireland Ltd that would make this transfer of data legitimate under section 11 DPA and Chapter IV of Directive 95/46/EC.

B. Reaction by FB-I and the DPC:

I welcome that FB-I has pledged to delete pictures that are delivered through “Akamai”. In our talks in Vienna FB-I told us that 90% of the pictures will be deleted “in minutes”, while it may take up to 45 (!) days to really delete pictures on the servers, this was not reflected in the reports.

This sounded great, but in reality I was not able to see a material change in deletion periods when testing random pictures. The deleted pictures were deleted after 4-7 days (!), none were gone earlier.

→ ***F122: While FB-I has pledged to have shorter deletion periods there was no factual change in random tests.***

The report has not at all covered the issue that Akamai is a US company, but not on the Safe Harbor. I have not received any arguments, evidence or files that indicate that the use of an external processor was covered under the law. Akamai is still today not appearing on the “Safe Harbor” list. However it grants itself very broad rights to process data going through its system further.

→ ***F123: There is no evidence that FB-I has deployed a sub-processor that is guaranteeing an “adequate protection” of the data provided to it.***

C. Legal Consequences described in the Original Complaint:

1. *There is no transparent notice that these bits of data are still held. In contrast to that, the user is told that the picture is “deleted”, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6 (1)(a) of Directive 95/46/EC.*
2. *There is no information in Facebook Ireland’s privacy policy that would substitute an accurate information of this process, as needed to comply with section 2D DPA and Article 10 of Directive 95/46/EC. This constitutes another breach of the principle of fairness in Section 2(1)(a) DPA.*
3. *There is no longer a legitimate purpose for holding on to these pictures. The data would have to be deleted according to section 2(1)(c)(i) DPA and Article 6(1)(b) of Directive 95/46/EC.*
4. *The further processing of this data is no longer relevant for the purpose of the processing, which constitutes a breach of 2(1)(c)(iii) DPA and Article 6(1)(c) of Directive 95/46/EC*
5. *The processing of the data is longer than necessary to fulfill the purpose. This would constitute a breach of section 2(1)(c)(iv) DPA and Article 6(1)(d) of Directive 95/46/EC.*

6. *It seems that there has never been an informed consent by the user to the use of these bits of data since the user just agreed to the processing by having the option to “delete” this content anytime. If Facebook Ireland does not remove any of this content, the consent seems to be neither informed nor unambiguous and therefore void under Section 2A(1)(a) DPA and Article 7(a) of Directive 95/46/EC.*

D. Additional Statement on the Legal Consequences:

Despite the fact that this point was already made in the original complaint I want to additionally highlight the following claim:

7. The processing and further use by “Akamai” seems to be in violation of section 11 DPA and Chapter IV of Directive 95/46/EC.

➔ ***R57: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

24. Complaint 21 “Groups”

A. Facts described in the Original Complaint:

The Facebook Platform gives users the possibility to “add” another user (“friends”) to “groups”. Groups are also displayed on the data subject’s Facebook page and the “news feed”. Data subjects do not have any possibility to prevent other “friends” from adding them to groups, other than not having friends at all. The membership in the group is fully active before the data subject even knows about its existence. There is no functionality that prevents unwanted adding to groups. The only option the data subjects are given is to leave to group, as soon as it sees it, but this may be too late.

In practice this means that the data subject may be added to a group that the user does not want to be associated with. Since groups can be “public” anyone on the internet can see the membership of a data subject in such a group. The only option the data subject has is to remove the tag after all this has already happened (opt-out).

That this practice is highly problematic can be with a Swiss group that was used for different forms of hate speech against foreigners. “Friends” of politicians and other public figures were added to the group without their consent. The politicians were questioned by the media about the group (see story in German, attachment 03).

To prevent other users from “adding” the data subject to the same group again, Facebook Ireland keeps the information that the user was a member of the group. This information is given when the user leaves

a group (see attachment 04). This means that the user can in fact never fully remove the relation to the group on the Facebook platform. All members are kept by Facebook Ireland, even if the user left the group.

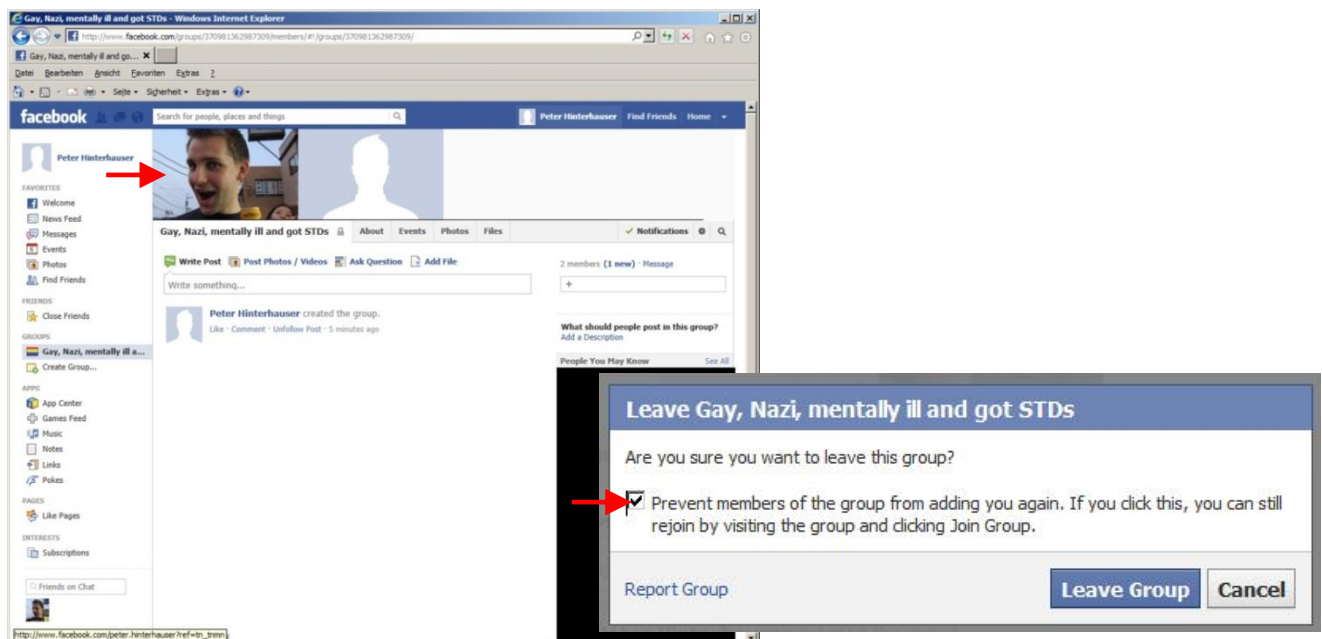
In summary Facebook Ireland processes personal data (group membership) without the specific consent of the user. General provisions in the privacy policy do not constitute a specific consent. The user knows that some friend might add him/her to some group, but this information is in no way substituting a specific consent. There is a major difference in the processing of different kinds of group memberships. Facebook Ireland does not add the users itself but it uses the personal data that is obtained without the specific consent of the user for its own purposes (e.g. aggregating the news feed, analytics about users).

B. Reaction by FB-I and the DPC:

There are groups that allow for damages to the reputation of the data subject. FB-I has changed some of the settings concerning groups.

Users now have an “invited” status, but as soon as they click on the Group for the very first time, they are turned into “members”. Just clicking at an invitation does not indicate the wish to join a group, nor does it constitute unambiguous, specific and informed consent.

The “invited” user is displayed in the head of the group, just like a normal member. There is no distinction that could prevent third parties that some user has something to do with the group. In addition just the fact of being invited to a group that is e.g. Nazi-related could form tremendous damage to a person in a country like Germany or Austria. There might be other topics and situations in other countries that could result in equal damage to the reputation of a person.



Screenshots: Users that were invited to the group “Gay, Nazi, mentally ill and got STDs”

When users have left a group, FB-I stores this fact to prevent them from being invited again. This was done without proper information to the user. Now there is some sort of information, but FB-I is not clearly saying to users that their former membership stays recorded when this box is not deselected.

Please refer to the solution I have outlined at “Complaint 02 – Tags” that also works for “groups”.

➔ ***F124: FB-I has made some (little) steps in the right direction which indicates that my initial complaints were justified, which I also derive from the ODPC’s analysis in the first report. Users can still be “added” without any action by the data subject, which by itself is processing of personal data without notice or consent, which might also harm the reputation of the user. Users turn into “members” without an unambiguous consent, simply by visiting the group.***

C. Legal Consequences described in the Original Complaint:

1. *There is no specific and informed consent by the data subject for the individual membership (opt-in). This constitutes a breach of section 2A DPA and Article 7(a) of Directive 95/46/EC. This would make any further processing illegitimate.*
2. *There is no transparent notice beforehand that former memberships are still held after the user clicked “leave”, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*
3. *If an opt-in system would be employed, there would be no need to keep information about former memberships. Keeping the information would then be illegitimate under section 2(1)(c) DPA and Article 6 (b-e) of Directive 95/46/EC.*

D. Additional Statement on the Legal Consequences:

I would like to amend my original complaint as FB-I has taken action in relation to the second claim listed above. However new version where “invited” people are shown on top of the group just like normal members is also incompliant with the law.

4. *The user is shown as if he would be a member of the group, which breaches the principle of fairness in section 2(1)(a) DPA and Article 6(1)(a) of Directive 95/46/EC.*
5. *FB-I is processing data that is added by another other third party. There is no way that FB-I could ensure that such data is accurate, complete and up to date. This breaches section 2(1)(b) DPA and Article 6(1)(d) of Directive 95/46/EC.*

➔ ***R58: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***

25. Complaint 22 “New Policy”

A. Facts described in the Original Complaint:

Facebook Ireland changed its privacy policy on September 7, 2011. The old privacy policy was from December 22, 2010 and lasted for just a little more than 8 months. The past years Facebook Ireland has renewed its privacy policy every year. Facebook Ireland did not amend the policy but rewrote it from scratch. It is almost impossible to compare the two versions and get a clear picture of the differences. In addition to that, Facebook Ireland was changing the policy unilaterally and without gathering consent or even giving prominent information.

In its (latest) privacy policy Facebook Ireland states:

“If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.”

According to section 2A(1)(a) DPA and Article 7 of Directive 95/46/EC the data use is only legitimate if the data subject has given an unambiguous, specific and informed consent.

There is no doubt, that the data subjects have never given such consent to the recent changes of the policy. There has not even been any form of action that could possibly be interpreted as consent.

Facebook Ireland might now argue that users have consented to the described regime of policy changes by consenting to the policy when signing up. Besides the fact, that this initial consent is generally invalid (see complaint 08) it seems that the consent to Facebook Ireland’s system of unilateral policy changes is especially questionable under section 2A(1)(a) DPA and Article 7 of Directive 95/46/EC. In fact this means that the user needs to permanently check on changes every time he/she uses facebook.com. The general “opt-in” rule, that means Facebook Ireland has to come after the user to get consent, is turned into a system where the user has to control Facebook permanently. This has the effect that the legal concept of section 2A(1)(a) DPA and Article 7 of Directive 95/46/EC would be undermined.

B. Reaction by FB-I and the DPC:

The report does not talk about the essence of the complaint and does not provide any counterarguments by FB-I. The report referred to an agreement between “Facebook Inc.” (the US parent company of “Facebook Ireland Ltd”) and the US Federal Trade Commission, as a reason why it did not deal with our complaint in the report. I understand that this agreement from November 29th 2011 was meant: <http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf>

However this agreement has nothing to do with my complaints against FB-I, since the ODPC and FB-I is of the opinion that FB-I operates independently from “Facebook Inc” as a separate controller for all users outside of the US and Canada. Agreements with the US parent company are not covering foreign subsidiaries that do not even cater to US consumers.

There is by definition no informed, specific and unambiguous consent to a policy that a user is not even aware of. FB-I has deployed different arguments during the change of the privacy policy this spring that were all rather absurd. Some of them were e.g. that “the media is informing the users anyways” or that they have placed “ads” on facebook.com to inform people about it. None of these actions guarantee that users are first of all aware and secondly agreeing to changes.

This is also what can be derived from many sections of WP 187 by the Article 29 Working Party, like e.g.:

“The specificity of consent also means that if the purposes for which data is processed by the controller change at some point in time, the user must be informed and put in a position to be able to consent to the new processing of data.” (WP 187, page 19)

C. Legal Consequences:

1. *There is no specific, informed and unambiguous consent by the data subject for any new policy after the user has properly signed up and given consent at this time (opt-in). This constitutes a breach of section 2A DPA and Article 7(a) of Directive 95/46/EC. This would make any further processing by FB-I illegitimate that was not covered by the initial policy at the time a user has signed up. FB-I might be able to find another ground for processing such data, but this must be assessed in each case.*

➔ ***R59: I hereby – involuntarily - request that the DPC to find that FB-I has violated the law and is continuing to do so. I ask the DPC to order FB-I to stop such processing.***