europe-v-facebook.org

RESPONSE TO "AUDIT"

by the Irish Office of the Data Protection Commissioner
on "Facebook Ireland Ltd."

Vienna, December 4th 2012

Table of Contents

I. Introduction

1. History of our Complaints

On behalf of "europe-v-facebook.org", Max 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.
We were not part of this public "audit" procedure and the ODPC says that it is totally independent from our "two-party complaints" procedure. Because the "audit" in fact overlapps with the substance of most of our complaints the ODPC has asked us, if the outcome of the "audit" solves any of our initial complaints. To answer this question we have now put together this "review of the audit".

2. Summary of this Review

We have dedicated extensive resources and time to analyze and evaluate the "audit" by the ODPC and the meaning for our complaints procedure. We hope this document will lead to a final and legally binding decision by the DPC in the near future and believe it is as a mile stone in this procedure.

We are happy to see that the "audit" has generally supported the facts we have brought before the ODPC. We were especially happy to see that we have no reason to correct any of our initial findings. A majority of FB-I's counterarguments were already expected and were even dealt with in our initial complaints.

We are 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 us this also indicates that our initial complains were fully justified.

At the same time we 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 we 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, we therefore hope that the facts we are submitting through this review will also lead to a reevaluation of the "audit" by the ODPC.

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

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

In many cases the “audit” has simply not covered major parts of our complaints. In many cases the “audit” only named one of the reasons why we believe that a certain action by FB-I is illegal, but did not elaborate about other arguments we submitted. This is reasonable 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 our 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 our 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/EG) 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. We recognize that a facultative non-binding “audit” procedure might not follow more stringent forms of proof, but we see this as necessary to decide on fundamental rights in a two-party complaints procedure. We 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. We are sure that by getting these additional information we will be in a position to solve these complaints.

In relation to all complaints the ODPC has still not given us access to any of the arguments submitted by FB-I. We were also not allowed to access files or evidence concerning our complaints. As expressed previously, we are left with almost no information in our own procedure.
This makes it factually impossible to have a “fair trail” 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 it calls for an especially firm, transparent and fair procedure. We have dedicated the entire second section of this report to the “procedural issues”.

In this section we have outlined in a more detailed way that we only seek access to information that somehow relates to our complaints, but we are not requesting such information on submissions by FB-I that only relate to the "audit".
We know that the current situation might be extraordinary for the ODPC and we are happy to resolve any misunderstanding in this relation. We very much hope that the section in this documents and the broad and overwhelming analysis of the situation will eliminate the deadlock that we currently face and lead the way to a legally durable solution.

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

➔ ***We are also unable to request a formal decision at this stage, because we lack the arguments by the other party as well as the majority of all files and evidence in relation to our complaints.***

4. Status of Complaints

In order to allow for a better overview we have indicated our status for all complaints in this table. As said before we see all our complaints as justified. Some complaints seem to be justified given the known facts, but this might change if we receive more information on the facts. We have also indicated where it is clear from the evidence that major material steps were already taken during the "audit".

Complaint 01	"Pokes"	**Complaint Justified**
Complaint 02	"Shadow Profiles"	**Further Investigation needed**
Complaint 03	"Tagging"	**Complaint Justified** *& Major Steps taken*
Complaint 04	"Synchronizing"	**Complaint Justified**
Complaint 05	"Deleted Postings"	**Further Investigation needed**
Complaint 06	"Posting on other Users' Page"	**Complaint Justified** *& Major Steps taken*
Complaint 07	"Messages"	**Complaint Justified**
Complaint 08	"Privacy Policy and Consent"	**Complaint Justified** *& Major Steps taken*
Complaint 09	"Face Recognition"	**Complaint Justified** *& Major Steps taken*
Complaint 10	"Access Requests"	**Complaint Justified** *& Major Steps taken*
Complaint 11	"Deleted Tags"	**Complaint Justified**
Complaint 12	"Data Security"	**Further Investigation needed**
Complaint 13	"Applications"	**Complaint Justified**
Complaint 14	"Deleted Friends"	**Complaint Justified**
Complaint 15	"Excessive Processing of Data"	**Complaint Justified**
Complaint 16	"Opt-Out"	**Complaint Justified**
Complaint 17	"Like Button"	**Complaint Justified**
Complaint 18	"Obligations as a Processor"	**Complaint Justified**
Complaint 19	"Picture Privacy Settings"	**Complaint Justified**
Complaint 20	"Deleted Pictures"	**Complaint Justified**
Complaint 21	"Groups"	**Complaint Justified** *& Major Steps taken*
Complaint 22	"New Policy"	**Complaint Justified**

II. Procedural Issues

Continuing from our previous communication we want to (again) comment on the very problematic situation we are facing with respect to the denial of access to files, evidence and arguments concerning the complaints proceeding against "Facebook Ireland Ltd" (FB-I). Because we lack essential information we are unable to claim our rights. It is particularly impossible to enforce our rights without getting all counterarguments, evidence and files in relation to our complaints. We 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/EG 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/EG 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 substantially 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 EU 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 seems to be in violation of Article 4 (3) of the EU treaty.

The current procedural obstacles make it actually impossible to effectively enforce our 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).

We have to stress that the DPC is a public, quasi-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 [we are] 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 us with the impression, that the ODPC does currently not see its crucial function regarding such rights.
Regarding our complaints against FB-I the DPC is the judicial tribunal which is deciding on the protection of our 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.

We have taken substantial effort to research our rights under the three legal regimes that govern the ODPC. We are hoping that this will help to overcome this situation and we hope the ODPC will grant us a fair and balanced proceeding. We also hope this will enable us 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 we are aware of the different legal system (common 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, we have invested substantial time to intensively research the Irish administrative law. After consulting different Irish experts we came to the following conclusions:

Two (overlapping) Proceedings

Our complaints are a two party procedure under section 10 DPA. After we files our complaints the ODPC has decided to start an additional public investigation ("audit"), which is based on other provisions and partly even based on agreements with FB-I.
Up to date we 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. We 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 our 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 our questions aimed at understanding which exact type of a state organ the DPC is. In an e-mail form the July 6th the ODPC has let us know that it *"never had to consider whether [it is] a Tribunal"*.
We have repeatedly expressed our view that the DPC is a "tribunal" (an administrative body that decides on civil disputes between individuals). We recently found that our view is shared in Irish literature [see e.g. Hogan/Morgan, 4th ed., 2012, page 156].
In addition we 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, we 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 such fundamental rights must be reached under a particularly formal, transparent, fair and balanced procedure.

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.

We 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/naturel justice. This is in contrast to previous claims by the ODPC that in such situations only the (little) statuary rights apply. In contrast to these claims, the Irish system requires public bodies to act beyond the statues 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 us full access to all files, evidence and arguments in relation to our complaints. 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/EG is not allowing such disclosure. We want to mention that according to our 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, we have not found a single member state that only offers a "two party" proceeding before the DPC, but does not allow such disclosure. We also suggest that the ODPC is awaiting the results from our letter to the Article 29 Working Party.

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 we want to name three:

First, the principle includes the direct duty of the tribunal to <u>disclose all relevant material</u>:
"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 bad 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 we are not getting the relevant evidence, arguments and files, but only the once the ODPC sees as "relevant" we are 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 we have submitted. Currently we 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 we want to mention that according to previous communication the ODPC has forwarded our complaints and the submitted evidence to FB-I. While we have made much of the complaints public on our web page, there were other parts that were not made public. To our 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 us repeatedly that FB-I's law firm ("Mason Hayes & Curran") has submitted very excessive and defensive material in relation to our 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 our position.

Appeals Process

During our visit to the ODPC on May 25th 2012 we were told by Gary Davis that all evidence, arguments and files would be presented to us when we 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 is not 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 his we were recently informed, that the Irish courts have so far ruled, that the appeal against the DPC is only on "points of law" and only on "serious and significant error of law" (see Novak v. Data Protection Commissioner, unreported).
We are uncertain that this very limited scope of an appeal is in line with Directive 95/46/EG, but for the matter of this document, we have to stress that if there is such a limited appeal the previous statements by the ODPC were false and misleading. Under such a limited appeal we would have no stage in the proceeding or the appeals process where we would have full access to these documents.

We have asked the ODPC repeatedly to at least name or grant us access to the unreported (!) "case law" that the ODPC is referring to when arguing procedural issues. Acceding to our research there is an obligation to disclose such material [see Hogan/Morgan, 4th ed., 2012, page 421f].

➔ ***We ask the ODPC again to send us the case law on procedural rights before the DPC and in an appeals situation.***

If the ODCP 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 we 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. We would also be unable to assess the chances of different legal moves. Such a situation is a textbook example of an unfair proceeding.

- ➔ ***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.***
- ➔ ***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 directly. We 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 "ever 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 trail") 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 "civil" or e.g. "administrative" matters and was interpreted convention-autonomously very broad, reaching into many fields that are traditionally "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 our 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/EG (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 our 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 field with a view to influence the court's decision"* [see e.g. "Niederöst-Huber v. Switzerland" p. 24, "K.S. v. Finnland p. 21" or "K.P. v. Finnland", 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. Finnland", 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. Finnland", p. 44, "K.S. v. Finnland", 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. Finnland, 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. Finnland", "Niederöst-Huber v. Switzerland", "Kugler v. Austria", "Ziegler v. Switzerland", "H.A.L. v. Finnland", "K.S. v. Finnland", "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]*

- ➔ ***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.***
- ➔ ***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.***
- ➔ ***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 the 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.

➔ ***The right to procedural safeguards, such as having a legal standing or receiving substantial information can also be derived from the ECHR, independently form 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. 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. The 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 [see (old) principle case law of the European Court of Justice e.g.: Heylens, 222/86; Johnson, 222/84].

The national procedures have to allow citizens of the EU to make the best possible case and allow for an effective remedy. While there is great latitude on how these principles are implemented, there must be an effective system in the member state. National law is to be interpreted in compliance with EU law.
If the ODPC is now depriving us to access all evidence, arguments and files concerning our 22 complaints, we are in a situation where an effective enforcement of our rights, that are based on Directive 95/46/EG, 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 criticizes of other member states from the possibility to make their best case.

➔ ***Summarizing a "draft decision" by the ODPC, where only hand-picked parts of evidence, arguments and files are referred to, is jeopardizing Irish compliance with EU law.***
➔ ***There is an obligation of the member states (and its public bodies) to interpret procedural law in a way that allows citizens of other member states to effectively claim their rights.***

E. 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 we 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 we want to stress that it cannot be bound by a pledge that deprives another party of constitutional rights.

➔ ***We hereby ask the ODPC to inform us about possible deals with FB-I concerning evidence, arguments and files in relation to our 22 complaints.***

Given the clear law in all three legal spheres that can be deployed in this case, we are asking the ODPC again to make clear which evidence, arguments and files were produced in relation to our complaints. From this on we 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 our complaints.
3. There might be some documents that only relate to the public investigation.

We accept that documents that only relate to the pubic investigation will not be disclosed and fall under Article 28 (7) of Directive 95/46/EG and the DPA (e.g. documents in relation to the "real name" policy of Facebook Ireland Ltd, which was not part of our complaints, but part of the "audit"). We hope that this view will also be shared by the Article 29 Working Party, which might deliver an opinion on the interpretation of Article 28 (7) soon.

We 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 we are accepting such limitations if necessary to protect legitimate interests. However, we would not accept general non-disclosure of files because of legitimate interests of others. Moreover, we expect clear and transparent communication about such limitations.

➔ ***Therefore we hereby (one more time) request copies and disclosure of all evidence, arguments, files and submissions that were produced for (1) the audit and our complaints ("dual purpose") or (2) in relation to our complaints only.***
➔ ***If the necessary documents are so far not produced we ask the DPC to produce the necessary evidence and files or request from FB-I their arguments.***

As a final remark we 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.

2. Principle against Bias / Decision on "complaints" during "audit"

The "audit" procedure was in fact mainly dealing with our complaints. In the first report from December 2012 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 our complaints, while sections 3.1 to 3.13 are related to our complains. This means that by the pages 80% of the chapters of the audit report are in some way dealing with our complaints.

The ODPC has expressed legal opinions on all 22 complaints before we were involved in a legal proceeding in any way (other than submitting the initial complaints). In summary the ODPC has already decided on our complaints before we were even (at least remotely) able to make our case. The DPC has even declared that to its understanding our 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)

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 our 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 our complaints. Despite our repeated efforts to contribute to the audit and our repeated requests to take part in the process we were not allowed to take part in any way, after filing our complaints. If we are 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 our 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 our complaints. In summary the ODPC is, when deciding about our complaints not only deciding about a dispute between "Facebook Ireland Ltd" and us, 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 now 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.

- ➔ ***We hereby ask the ODPC which officer will factually work on our complaints?***
- ➔ ***We hereby ask how the ODPC will ensure that an unbiased decision will be delivered?***

III. MATERIAL ISSUES

1. General Remark: Article 29 Working Party Opinions

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

First of all we 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/EG 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/EG). While the published opinions of the Working Party are not legally binding, they must be seen as guiding line by the member states, everything else would make this institution obsolete.
In addition we also understand the opinions to be the common understanding within the EU of the meaning of Directive 95/46/EG. Since the national law has to be interpreted in line with EU directives, we 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 ODPC 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 we believe that FB-I should at least be compliant with the relevant working papers, since they represent the common understanding of a "minimal standard". Some working papers also suggest different options which would lead to compliance. Since the ODPC and FB-I follow a "best practice" approach we would expect that such suggestions would be taken into account in their most stringent form. Anything else could hardly be "*best* practice" but would rather be just "*some* practice".

We have very much welcomed that the ODPC has partly followed WP193 when dealing with the "facial recognition" tool by FB-I. At the same time we could only see very little reference to other working papers that seem relevant to our complaints. We have decided to bring these documents in, since they could possibly be helpful when solving different legal questions. We would be very happy if the ODPC 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.

- ➔ ***We generally assume that 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.***
- ➔ ***A "best practice" solution cannot possibly be below the minimal level outlined in the relevant WP. Instead it should follow the suggestions in the most stringent form.***
- ➔ ***We hereby ask the ODPC to outline when and why it departs from this common understanding, whenever we have referred to a specific WP.***

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 1.5 years, we want to make a couple of remarks on this issue:

A. Relation "Facebook Inc. (USA)" / "Facebook Ireland Ltd."

While our 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, we have to mention that during the last 1.5 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.
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 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 (Facebook is said to make use of what is known as the "Double Irish Agreement" that allows to push cooperate taxes down to about 2-3%).
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. We have serious doubts that FB-I might in fact not be freely deciding about the operations of facebook.com, but given the limited information we are currently not claiming that FB-I is not the controller. At the same time we would very much hope that the ODPC can deliver some fact based evidence to make sure we are running a procedure against the right entity.

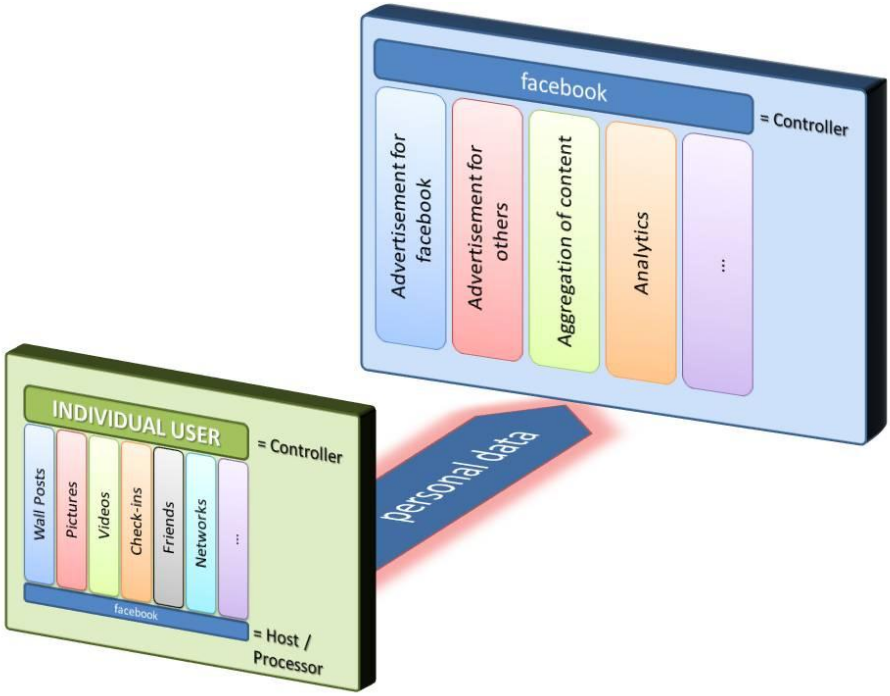
➔ ***We would welcome if the ODPC could produce or deliver fact based evidence that ensures that FB-I is actually the factual controller of facebook.com outside of the US and Canada.***

B. Relation Users / Facebook

Split Responsibilities and Powers

As we have outlined in our initial complaints, we have dealt with the question of the controller in detail and found a solution which we 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/EG are applied to this form of a system, it is clear that we have 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.

We 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).

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 our 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 1.5 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 we want to cite the original statement from Robert Ardelt, 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 Datenschutz-richtlinien 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. We are using the English term "control" to explain that we are 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..." (Livestream at 11:30, See Copy on YouTube)*

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 out 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 trigged 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.

➔ ***We hereby ask the ODPC to send us any arguments, files or submissions that indicate other facts.***
➔ ***We have no reason to believe that our analysis in the initial complaint is false.***

C. Household Exemption

In a final remark we also mention that the report has departed from WP163 when it comes to the rights and duties of the users. We 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)*

We 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).* 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)*

➔ ***We have no doubts about our initial analysis and ask the ODPC to deliver a solid assessment.***

3. General Remark: Technical Report

Both reports are accompanied by technical sections. These reports are generally in line with our findings and seemed to have produced reasonable outcomes, which is why we see our 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 we respect the confidentiality of certain trade secrets of FB-I or security relevant information, we cannot base our proceeding on such findings.

➔ ***We 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 our initial complaints.***

➔ ***We understand that it might not be possible to disclose certain information, that is e.g. covered by trade secrets or information that would allow circumventing FB-I's security systems.***

In addition we want to mention that we were 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 first analysis. The webpage of "FTS Solutions" 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.

➔ ***We hereby ask the ODPC to give us a rough idea about the background of "FTR Solutions".***

4. Complaint 01: "Pokes"

The December Report 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". 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."*

We were 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 not informed about how FB-I has changed or was intending to change the processing of "Pokes".

Neither the DPA, nor Directive 95/46/EG 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 we 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 only substantial counterclaim of FB-I why pokes are kept for an indefinite time ("poke harassment") is surely creative, but legally absurd.***

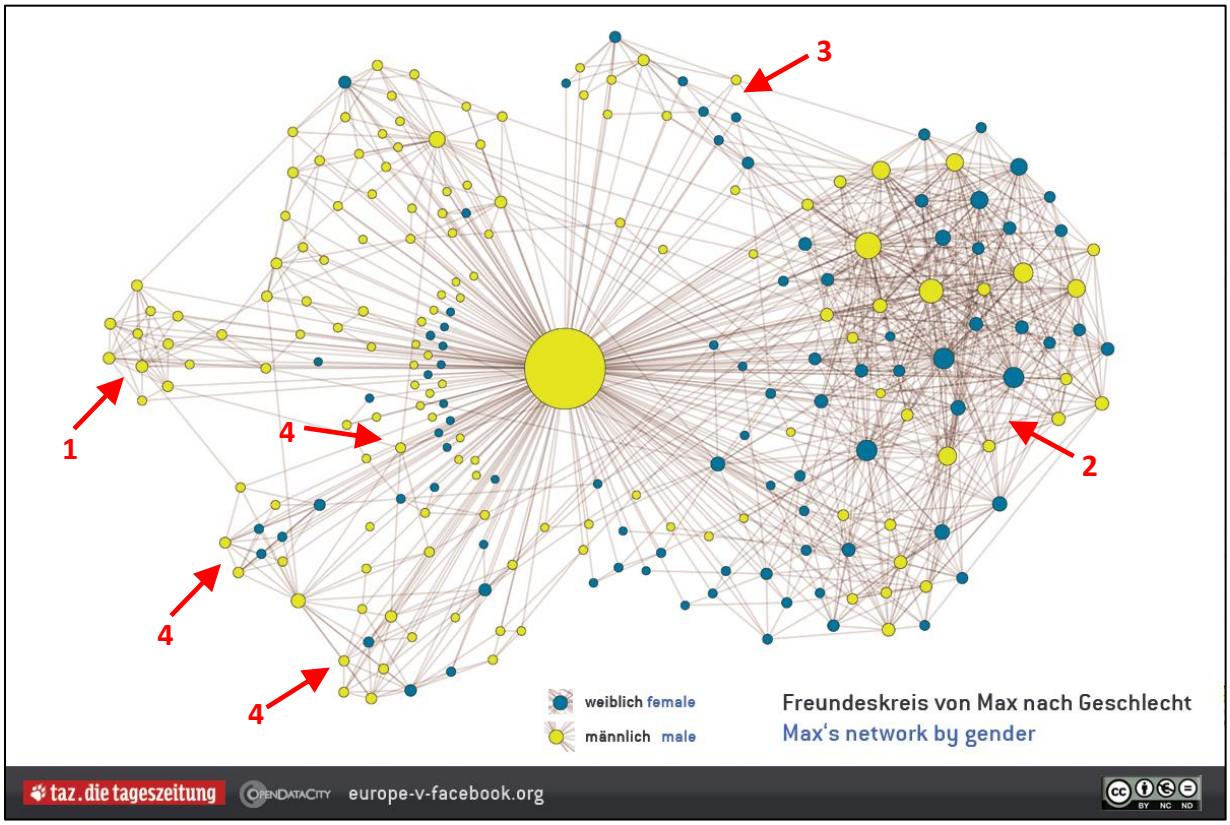
The fact that FB-I has stored information, without a legitimate purpose and without a justification, without proper information and for an indefinite time constitutes a clear breach of the provisions of the Irish DPA and the Directive 95/46/EG as described in our Complaint 01 from August 18th 2011.

➔ ***We ask the ODPC to investigate how "Pokes" are treated by FB-I after the complaint was launched and disclose all information that FB-I has delivered on this issue.***
➔ ***We ask the ODPC to ensure that this illegal processing of data is not conducted further and all old "poke" data is deleted.***
➔ ***If no other arguments, evidence or files are before the ODPC, we are now reassured that FB-I has been in breach of the law and that our complaint was therefore fully justified.***
➔ ***To show that a breach of the Irish law is not without consequences, to prevent other companies in Ireland and the EU to breach the law as well and to show that international companies are not above the law we hope that the DPC will impose a substantial penalty.***

5. Complaint 02: “Shadow Profiles”

After researching the findings in both reports and the technical analysis, we 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 we 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 we were unable to further specify the issue, but we are now able to do so:

As an example we want to submit the graphic below. It combines Max Schrems’ 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. In reality there are additional “hidden” connections to many more users (e.g. by searches, imports, address books, click data) and every dot is not only a name,

but again a whole Facebook profile. In addition to these profiles and connections, hidden click data, advertisement information or data from social plugins can be added to every dot.
The result is what is 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"). For doing so the "visible" data is connected with "invisible" data that might serve another purpose (e.g. protocols, IPs, friend finder data, administrative data, data of others). This allows for profiling on people that have never really shared anything on facebook.com, or are not even a member of the platform. This practice seems to be the background of what we called "shadow profiles" in the initial complaint. In essence, 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.

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 become 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)*

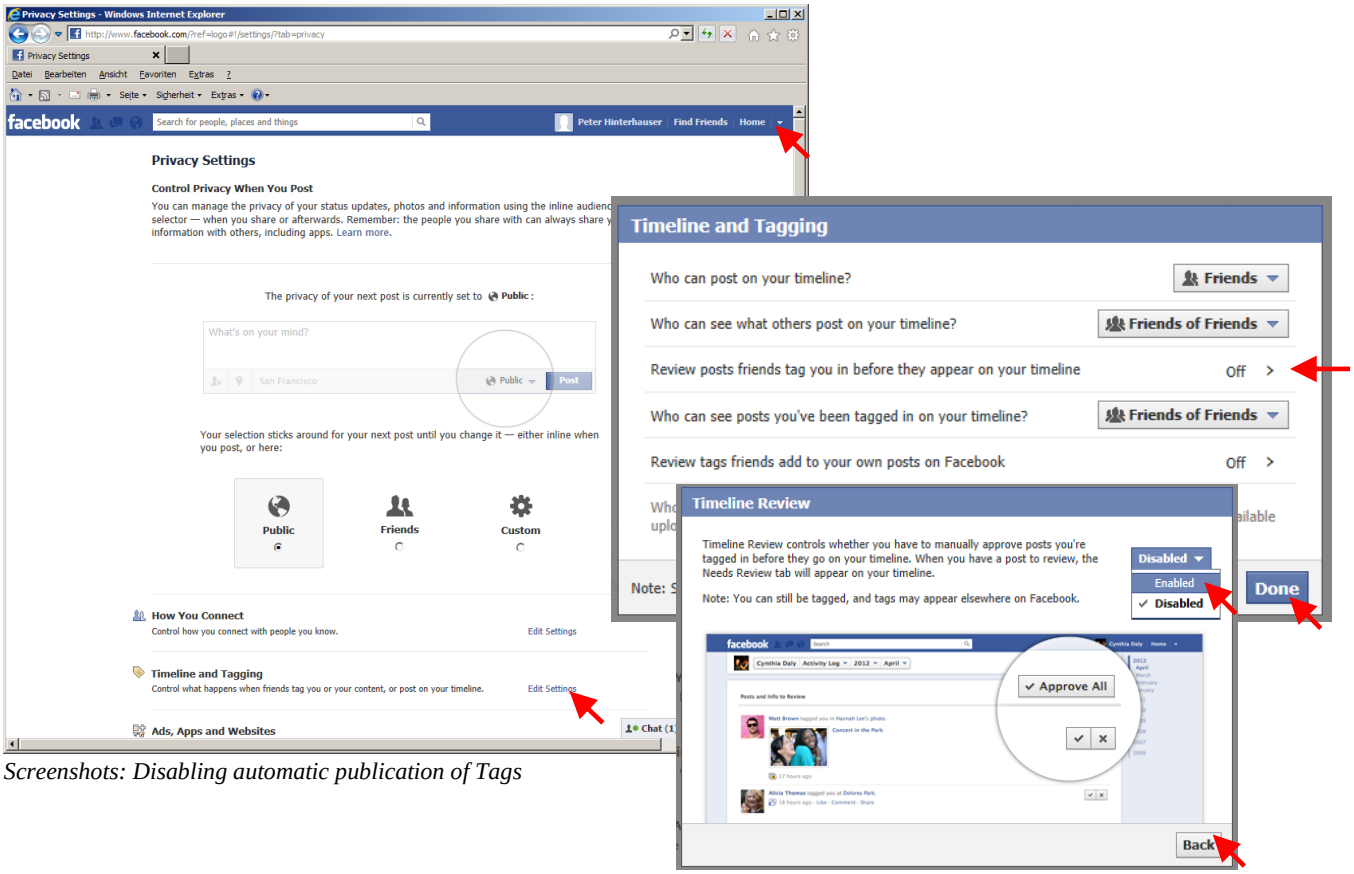
This does not say, that FB-I does not use other, less obvious, information to target ads, promote their service or suggest "friends".

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. Our Complaint 02 clearly names the "friend suggests" as only one of many possible results of these extensive profiles.

- ➔ ***We cannot elaborate further, because of the lack of evidence, arguments and files in relation to this complaint.***
- ➔ ***Therefore, we ask the ODPC to investigate if and how such processing of data takes place and disclose all information that FB-I has delivered on this issue and investigate further to determine if the complaint is justified or not and get back to us with the results.***
- ➔ ***Currently we have no reason to believe that our initial complaint is not justified, given the doubts above.***

6. Complaint 03 “Tagging”

We welcome that 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 ,however, allow disabling tagging itself. It does also not change the removal of tags. FB-I still keeps all “removed” tags.

- ➔ ***The new system allows to prevent automatic publication of tags (a step in the right direction).***
- ➔ ***The system is in fact an “opt-out” from automatic publication and is well hidden.***
- ➔ ***There is no change in relation to the removal of tags and the fact that FB-I keeps even the “removed” tags.***

The ODPC has changed its position from the first report towards the review: While in the first report it has claimed that there must be a possibility to fully turn off tags, 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 we are not requiring an ability to prevent Tagging at this time." (Review, page 48)*

Only some numbers from the United States (!) that indicate that only some people remove tags seemed to be new evidence. We cannot understand why the ODPC has changes its position.

- ➔ ***We hereby ask the ODPC to explain this change of position.***
- ➔ ***If any arguments, files or evidence was not disclosed in relation to this change we hereby ask the ODPC to deliver such documents.***

The reports are not covering all the issues of you initial complaints, 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", but without any affirmative action by the data subject, just because people may say "no" later. The report is 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.

- ➔ ***There is no affirmative action that can possibly constitute "specific" and "informed" consent.***
- ➔ ***The data is processed even after the "removal", therefore FB-I does not even provide an "opt-out".***
- ➔ ***Also tags that had to be "reviewed" are kept after they are removed.***
- ➔ ***We hereby ask the ODPC to produce or disclose evidence, files and counterarguments in connection with the initial complaint. Currently we see ourselves reassured that the original complaint was fully justified.***

Currently there is only one solution which we would understand to be fully compliant with the law. This solution is by the way the standard procedure with "invitations" or "adding" people in just about all other systems we know of and should be deployed with tags, groups, events and other "objects" that data subjects get connected to by others:

Step **1**: A third party can establish a link between a data subject and an object.
This link stays invisible 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.

- ➔ ***This solution is a standard practice and the only known system that is compliant with the law.***

7. Complaint 04 “Synchronizing”

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. We took a closer look at these investigations and came to the conclusion that the Canadian DPC was in essence referring to the solution by 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 e-mails and that FB-I only uses e-mail 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 e.g. using the subject “Check out my photos on Facebook” for this message – the test account we were using 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. Only the recipient and a small portion of the message (underlined in green) are chosen by the user that is sending the invitation.

Screenshot: Invitation and Opt-Out Link

We therefore question FB-I's claim not to be sending the message themselves and not to be the controller. In essence they are deciding about the content (even false content). The inviting user does not even see the subject or the content of the message. 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 at least "joint controller" for such invitations.

➔ ***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.***

➔ ***FB-I cannot shift the responsibility to the user, yet shift the advantage to itself.***

Agreement with the Hamburg DPC

The solution that was reached by the DPC in Hamburg was surely a big 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, we can totally eliminate the idea of consent based processing. This form of consent is the total opposite everything that can be read in any data protection 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, we have no doubts that there is no "unambiguous" consent when data subjects to not react to an e-mail. Otherwise there could be some claim in any spam e-mail that would allow using all personal data of the recipient.

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.

➔ ***Inaction following an e-mail does never constitute informed and unambiguous consent.***

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. Volker und Markus Schecke v Land Hessen*)? 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 gänzliche Verzicht auf das Importieren von Daten Dritter, waren in den Verhandlungen nicht zu erreichen. Sie dürften auch aus rechtlichen Gründen kaum durchsetzbar sein."*
> ***Translation:** „A broader solution, 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 was uncertain if he has 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 not the result of a formal procedure that was applying the law to FB-I but the result of a "trade" where FB-I had the much better cards.
We are 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".

- ➔ ***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).***
- ➔ ***FB-I was not able to deliver any material counterarguments.***
- ➔ ***We ask the ODPC to deliver any counterarguments, files or evidence concerning this matter.***
- ➔ ***Therefore we have no reason to believe that our initial complaint is not justified.***

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 report and the technical analysis only lead to a "geo block" of users in the EU/EEA. We are 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. We 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.

- ➔ ***FB-I was not able to deliver any material counterarguments.***
- ➔ ***We ask the ODPC to deliver any counterarguments, files or evidence concerning this matter.***
- ➔ ***Therefore we have no reason to believe that our initial complaint is not justified.***

8. Complaint 05 "Deleted Postings"

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 Max Schrems has deleted these postings at approximately 12 days before the "access request". We are uncertain 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).
We 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?

- ➔ ***Therefore, we are asking the ODPC 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.***
- ➔ ***We ask the ODPC 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.***
- ➔ ***We also want to get a stringent explanation how only certain postings ended up in the file.***

Written by Max Schrems:
Either way the claim 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 before that and the last time during the first half a year of 2011. I can recall this because this was before and during my studies abroad.
While I cannot recall the exact times, I hereby assure that I have deleted all of my Facebook "wall" repeatedly and way before the 90 day period that FB-I claims.

- ➔ ***We ask the ODPC to get solid proof which would support FB-I's claim that the postings were deleted only 12 days before the filing of the access request or before the production of the data file which "Facebook Inc." (the US parent of FB-I) has sent to Max Schrems.***

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 Max Schrems has used the automatic script for the very first time in 2010. This would have been way before the 90 days and would surely include postings from 2008 and 2009. The claim by FB-I seems to be false and misleading.

- ➔ ***In essence we are asking the ODPC to investigate the exact circumstances and get back to us with the exact arguments and solid evidence for FB-I's counterarguments.***
- ➔ ***Currently we have no reason to believe that Complaint 05 is not justified, given the doubts above.***

9. Complaint 06 "Posting on other Users' Pages"

We are 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 we have nothing further to add at this point.

➔ ***FB-I has changed towards a model that we suggested in the initial complaint.***
➔ ***Therefore we have no doubt that our initial complaint was justified.***

FB-I's new solution also has a drawback that we 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 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 thorough 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.
This is undermined since the "owner" of the page (*mind: FB-I currently claims to be the controller of facebook.com*) can switch the postings from "friends" to "public". Making any comment viewable and searchable for anyone in the world. This is the assessment of the ODPC:

> *"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)

We cannot share this position, since it was the core idea and supported by the ODPC that users should get this information in order to make informed decisions. It is not stringent to now claim that users do not post data with the expectation that this post will only be shown to a restricted audience.

> 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)

This 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 we could shred the whole proceeding against FB-I, since in the end all users have the option not to use the service. It is the essence of data protection law to allow people to use new technology and be able to trust it.

➔ ***We cannot share the view of the ODPC in this respect and think our initial complaint is justified.***
➔ ***We hereby ask the ODPC to disclose all documents that relate to this complaint.***
➔ ***In addition we urgently ask the ODPC to name the provision of the Irish Data Protection Act from which it has derived this "simple solution", since we were unable to find it.***

10.Complaint 07 “Messages”

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 we 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)

We want to stress that FB-I was able to deliver all messages that were deleted when supplying Max Schrems 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 we 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.

➔ ***FB-I is able to retrieve all deleted messages from the system, no matter where they are stored.***

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. We cannot see any facts or material arguments that would support this claim in the reports or the technical analysis.

➔ ***We could not find any fact based evidence that messages are deleted when all users have deleted their individual copy of the message.***

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.”*

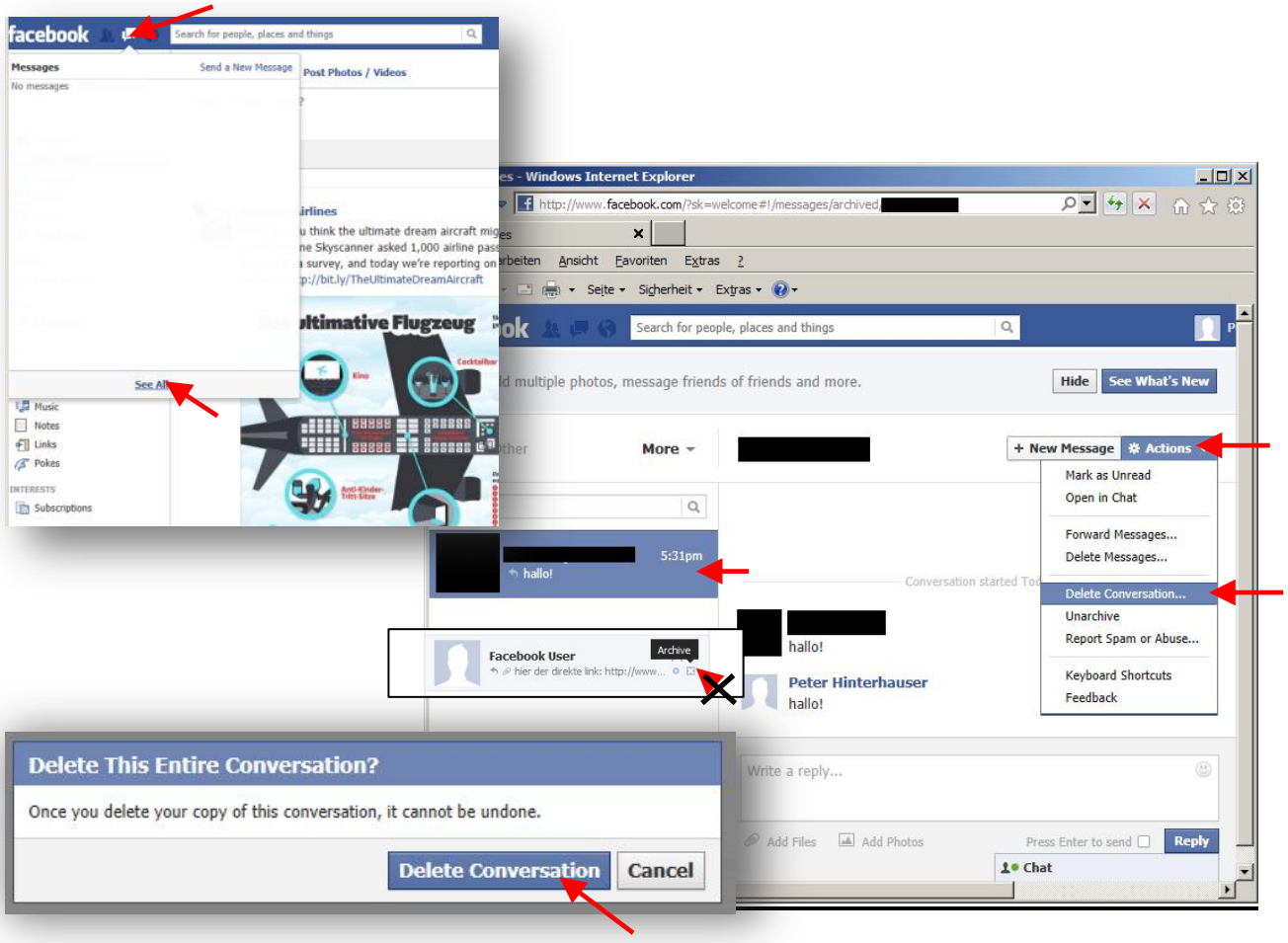
➔ ***There is no fact based evidence of the extent of processing of the content of messages.***
➔ ***FB-I’s own privacy policy does not limit the use of content of messages for specific purposes.***
➔ ***There is fact based evidence that non-content data is not used.***

The Material Claim

Independent form these factual problems the reports have not dealt with the material claim in the initial complaints 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.

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 if would take hours. There is no way for "mass deletion" and FB-I does not automatically "delete" old chats, like every other chat system we are aware of. The merger between "chats" and "messages" has further lead to a system where every little exchange is treated like highly relevant personal mail. This does not reflect the users' reality and is an exceptional approach that cannot be seen anywhere in the world.



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

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

➔ ***There is no standard deletion and no option for mass deletion.***

Comparison to E-Mail and Chat Programs

If this is compared to e-mails we want to stress, that e-mails donnot 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 the data set of Max Schrems 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 e-mails.

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.

➔ ***FB-I's chat system can in no way be compared to other systems that offer similar functionality, since these systems do not allow to centrally retrieve old, deleted messages.***

Government Access

In addition FB-I is legally obliged to disclose such 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.

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 (possibly unintentional) "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 we 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/EG.

➔ ***Therefore we have every reason to believe that our initial complaint it fully justified.***

➔ ***We ask the ODPC to disclose all files, evidence and arguments on this complaint and make FB-I produce a material counterargument.***

➔ ***We would not sport a penalty, since we believe this happened without any negligence by FB-I.***

11.Complaint 08 “Privacy Policy and Consent”

A. Privacy Policy

Old Policy: Since we have filed our initial complaints in August 2011, FB-I has changed its privacy policy twice (!) and there is a third change on the way. We want to point at WP187 and the original complaints concerning the level and form of information, which especially very complex systems have to be accompanied with (see WP187 page 21).
The claims FB-I has submitted to the ODCP concerning the old policy seem not stringent to us. The report has only cited claims by FB-I that our claims are wrong, but the report does not deliver any material arguments by FB-I. From the current level of information we cannot see that any material counterarguments were brought forward concerning our initial complaints.
Because of the limited information we got through the report, we cannot really respond to the counterarguments to what we have brought forward concerning the content of the old privacy policy. But we understand the ODPC’s findings in the report of December 2011 to be very much supporting our view and see nothing that would be contrary to the claims in our initial complaint.

- ➔ ***We ask the ODPC to disclose all arguments, evidence and files in relation to FB-I’s counterarguments. We face total absence of material counterarguments by FB-I.***
- ➔ ***We are still of the view that FB-I’s old policy could not constitute a valid legal basis for the processing of our data under the DPA and Directive 95/46/EG.***
- ➔ ***If there are no other arguments than the ones named above, we are of the view that our complaint was justified in relation to the previous policy.***

New Policy: We very much welcome 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 a year, it is still not possible for the members of our group to exactly say what FB-I does or does not do with users’ data, based on this policy.

We 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.

We welcome the approach of “inline” consent for every function. We have ourselves 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.

The first report by the ODPC of December 2011 has to our view outlined many important things concerning the current policy. We especially want to point at the findings on pages 39 to 41. When

looking at the changes by FB-I and the review, we 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.

We are 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/EG. We have summarized some issues as examples why we are still of the opinion that this cannot be the basis for a valid consent:

a. We believe FB-I has to clearly say or list what they do with our 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 translates 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

> *"We may use your data in relation to everyone we interact with (half of the internet)."*

This is maybe the most abstract (and therefore the most unlimited) 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 opinion we know, including WP187, pages 19f.

On top of this, the policy also claims that users consent to future developments of facebook.com. 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 "module" policy system that allows to get 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. We 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. We 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. FB-I has to delete all data the users have previously "removed" or "deleted". It seems like the deleted data we have discovered in 2011 is still on FB-I's servers and only data that was deleted after the changes are in fact deleted.

i. After it was discovered that "deleted" information was still kept by FB-I they simply relabeled 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 form deleting data. We 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.

j. 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.

k. 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; we are 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 we were 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.

l. FB-I has to take back the change that allows them to keep users' information after users have deleted their accounts. FB-I goes even further on this in the recently proposed third version of the new policy.
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. We 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).

m. 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 holes 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").

n. We believe FB-I has to take back the change that makes the user responsible for getting back 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.

o. We 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.

p. 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.

q. 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).

r. FB-I works mainly with 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. We believe that FB-I has to highlight processing that cannot be reasonably expected, instead of rather obvious processing.

As said before, the issues listed above are only some examples. In general FB-I's privacy policy is a lengthy document, that has endless 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 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 we have filed our initial complaints, despite having a very "flexible" policy. So this argument seems to lack any substance.
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, this can therefore only constitute informed and specific consent for these specific operation.

Overall we believe that FB-I has to draft a totally new policy. We suggest there is on section for the core features and additional sections for additional features that users consent to opting into such features. 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".

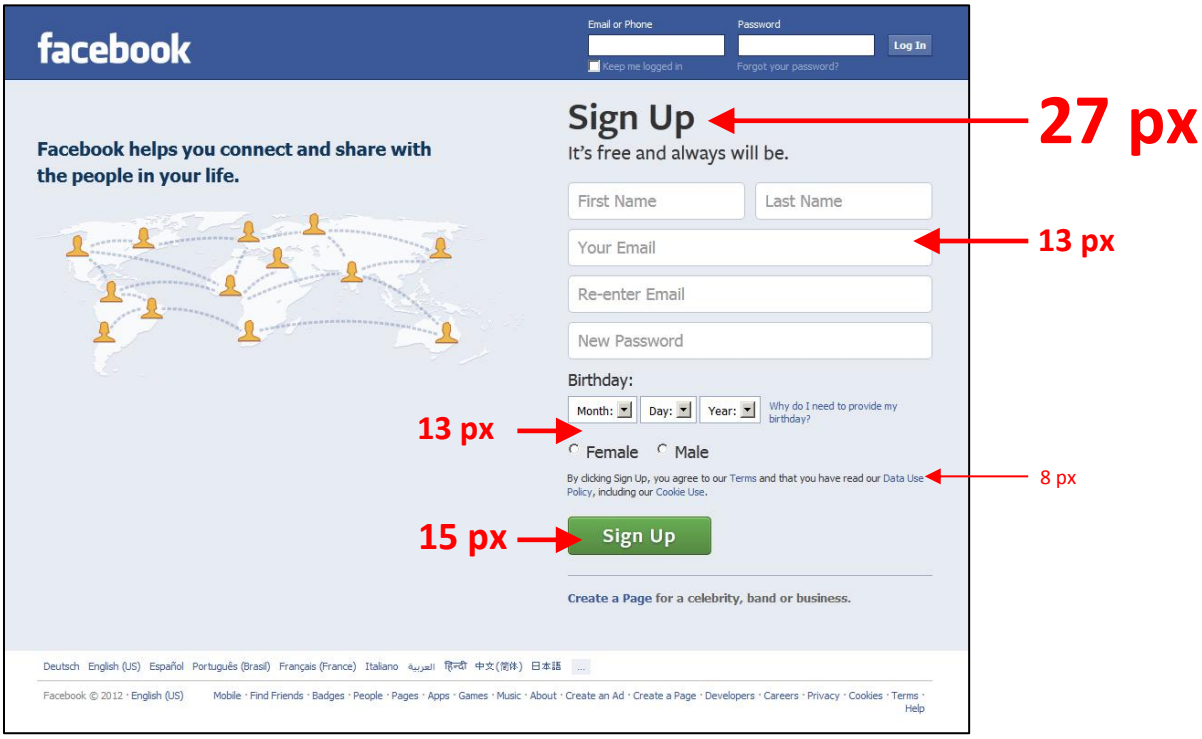
- ➔ ***We ask the ODPC to get a clear statement on who is the controller of every operation on facebook.com and what FB-I means by when saying the users' data "belongs" to the user, when they are at the same time not letting the user be the controller over "their" data.***
- ➔ ***We ask the ODPC to disclose all arguments, evidence and files in relation to FB-I's counterarguments concerning the new and old privacy policies.***
- ➔ ***We ask the ODPC to have FB-I produce a list of all data categories and explain the exact, specific purposes for which this data is uses (see also "Complaint 10 – Access Requests")***
- ➔ ***We ask the ODPC to review FB-I's new privacy policy in line with the claims listed above.***
- ➔ ***Given the issues brought forward above, we are sure that Complaint 08 is justified in relation to the new policy as well.***

B. Consent

Old Sign-Up Process: We welcome that the ODPC has made FB-I change its sign-up process towards a new system that gets much closer to what we have outlined in our initial complaint. 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 fact that this means that users that signed up previously have not given a valid consent. We are still of the view, that FB-I does currently not have a valid consent by users that signed up before this change. Mind, that this still allows FB-I to operate under other provisions of the DPA and Directive 95/46/EG (e.g. performance a contract).
FB-I is cited repeatedly in the report form December 2011 to claim that the ongoing use of facebook.com would constitute informed, specific and unambiguous consent to the (old or new) policy. We are 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).

- ➔ ***In substance FB-I deployed arguments we cannot share. We are still of the view that there has been no valid act of consent. FB-I would have to ask all existing users for a new and valid consent.***
- ➔ ***If there are no other arguments than the ones named above, we are of the view that our complaint was justified in relation to the act of consent under the old sign-up process.***

New Sign-Up Process: We 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).



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

We still question if this small link can really constitute an informed, unambiguous and specific consent, given the large amount of very problematic and complicated data processing FB-I engages in. The solution is surely a step ahead, but "best practice" would be at least a check box, which is seen to be necessary for any form of consent in many member states. 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 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.***
- ➔ ***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".***
- ➔ ***The ODPC did not touch on how "free" consent on facebook.com really is. FB-I did bring forward any counterarguments. We ask the ODPC to produce and disclose such documents.***

C. Improved Information for new Users

We 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 picture 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."*

We are 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.

- ➔ ***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.***
- ➔ ***We 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 an unambiguous consent.***

12.Complaint 09 “Face Recognition”

We 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/EG. This was very clearly stated in WP163 issues by the Article 29 Working Party. The procedure has shown to our 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). We 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.

We also want stress that the ODPC has not dealt with the other provisions of the Irish DPA and Directive 95/46/EG 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, we 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, we 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”.

We are waiting to see how the new system will be designed that only recognizes faces of users that have previously consented. 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. This seems also to be unclear in the current situation: How does FB-I guarantee that a photo of a data subject living in the EU that is e.g. uploaded in South America is not processed by the facial recognition tool? Given the experiences mentioned above will also have to see how FB-I is exactly getting a valid consent when redeploying this tool in the EU/EEA.

“EU” and “EEA” are also the key words for the last remark we 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/EG 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 we are 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.

- ➔ ***We welcome the new approach, but believe that the ODPC has to ensure that an unambiguous, specific and informed consent is necessary under the law (not just under a “best practice” approach).***
- ➔ ***We ask the ODPC to figure out how FB-I is currently distinguishing between users form the EU/EEA and other users and how FB-I is intending to do so between users that have and have not consented to facial recognition.***
- ➔ ***We ask the ODPC to also elaborate over the other principles that govern processing of data.***
- ➔ ***We are making the ODPC aware that it is responsible for all users outside of the US/Canada and that all these users have the same rights under EU (and Irish) law.***

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 the initial access request by Max Schrems 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 we would have expected that this issue would be prioritized and investigated in an especially transparent and detailed way. Instead we had to find that the exact opposite seemed to have happened, which is also supported by the facts we had to find when looking at the current "solution" to access requests.

A. The ODPC's Reports and Investigation

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.

The report claims 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."* In this relation we want to mention that 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, which would surly have limited the amount of people that made requests to only the ones that really wanted to get access. It seems hypocritical to first tear down the only limitation to then complain about an "extreme" number of requests. We believe that FB-I was simply unable or unwilling to additionally process the payments by thousands of users and therefore waived the fee in its very own interest.

➔ ***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.***

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 us, 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, we are 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.

➔ ***The ODPC has illegally "waived" a statutory obligation of FB-I and allowed it to break the law.***

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 our complaint ("10 – Access Request"), the ODPC has not made any evidence, argumentation or

legal analysis public. We 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.

➔ ***Therefore we ask the ODPC hereby to disclose evidence, arguments and files in relation to the existence and legal qualification of (personal) data on FB-I's systems.***
➔ ***We hereby ask the ODPC to disclose in detail the methodology that led to the ODPC's finding, how the fact finding was conducted and explain the legal analysis which led to the published results.***

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. We 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 we have submitted.
The ODPC has let us know that is has taken account of the 19 data categories we have listed in our initial complaint. We have repeatedly pointed out that this was *not* an exhaustive list of data categories and that we expected the ODPC to investigate into other data as well. We have even offered to submit a second list of data categories that we have collected after the initial complaints. The ODPC has not gotten back to us on this proposal. We currently have evidence of about 20 more categories.
During our talks with FB-I in Vienna, the representatives of FB-I have declared that the 19 categories we 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 we 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 we are giving access to – I think it is a terrific tool and we are constantly working. You know it's not easy!"*

Therefor we do not believe that the ODPC has found all data categories. We are sure that the data categories listed on pages 64-65 of the first report do not represent all personal data held by FB-I. 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 report lists e.g. "photos", but there are also IPs, Dates, EXIF data or tags attached to pictures these sub-categories are not listed in the report.

➔ ***There is evidence that the list of data, published in the ODPC's reports, is incomplete.***
➔ ***We hereby ask the ODPC to disclose the methodology and evidence used to derive this list.***

The ODPC has repeatedly said that is 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 we discovered and described below (see section "C. Self-Service Approach" below) we are 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, we are very much worrying about the quality of the investigation into other issues (e.g. the investigation on other, so far non-disclosed data categories).

➔ ***How could the ODPC overlook that the "tools" where in fact not working properly?***
➔ ***How can the ODPC guarantee that other questions of fact were properly examined if even such basic problems were not discovered by it?***

B. Facebook's Credibility relating to Access Requests

In order to demonstrate that FB-I has so far repeatedly lied and made obvious false claims we want to copy four of the many e-mails FB-I has sent to us 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 e-mail 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 e-mail 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 we are 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 us 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.***

Conclusion – Facebook's Credibility relating to Access Requests

Given this record there is no reason why we 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.

➔ ***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.***
➔ ***We hereby ask the ODPC to disclose all evidence, arguments and files that were produced in relation to the existence of data categories on FB-I's servers and the question whether they constitute "personal data" or not.***

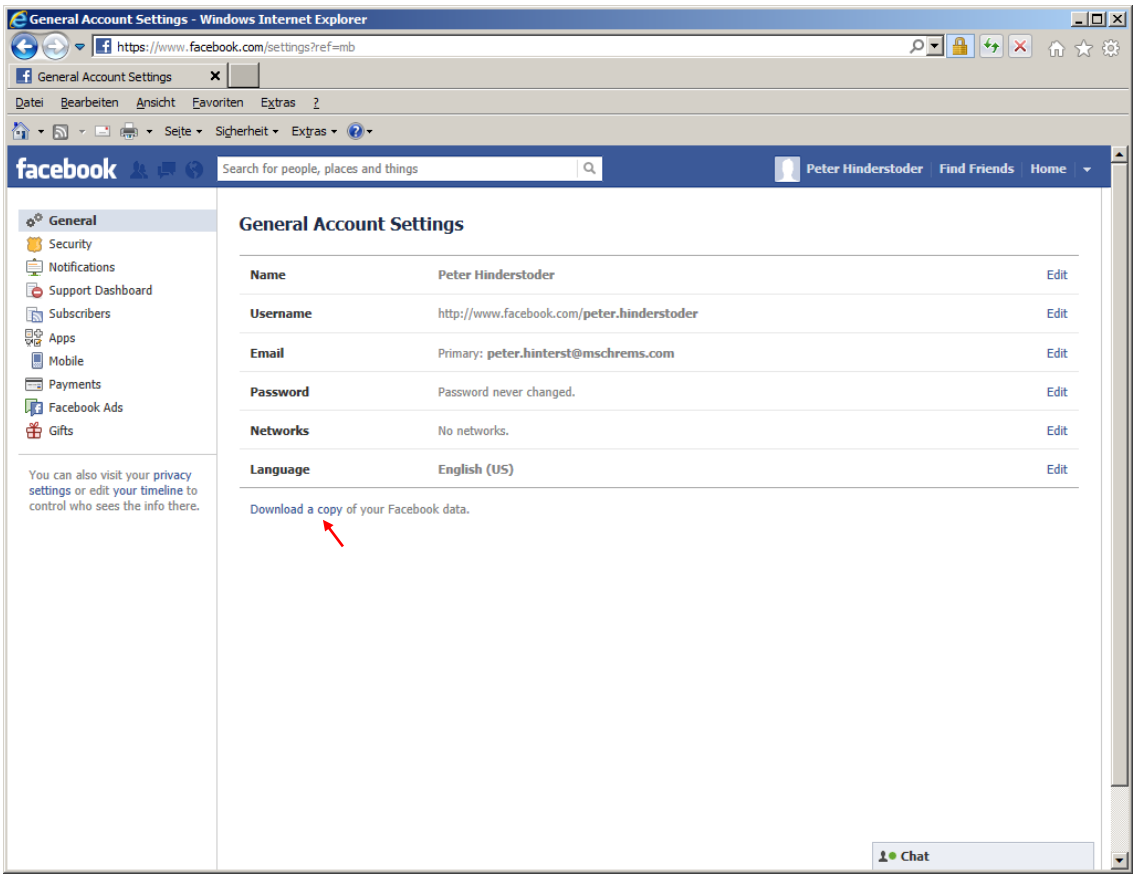
C. "Self-Service" Approach

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. We have been very critical of this approach, since these tools replaced the standard response.
We 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 we 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.

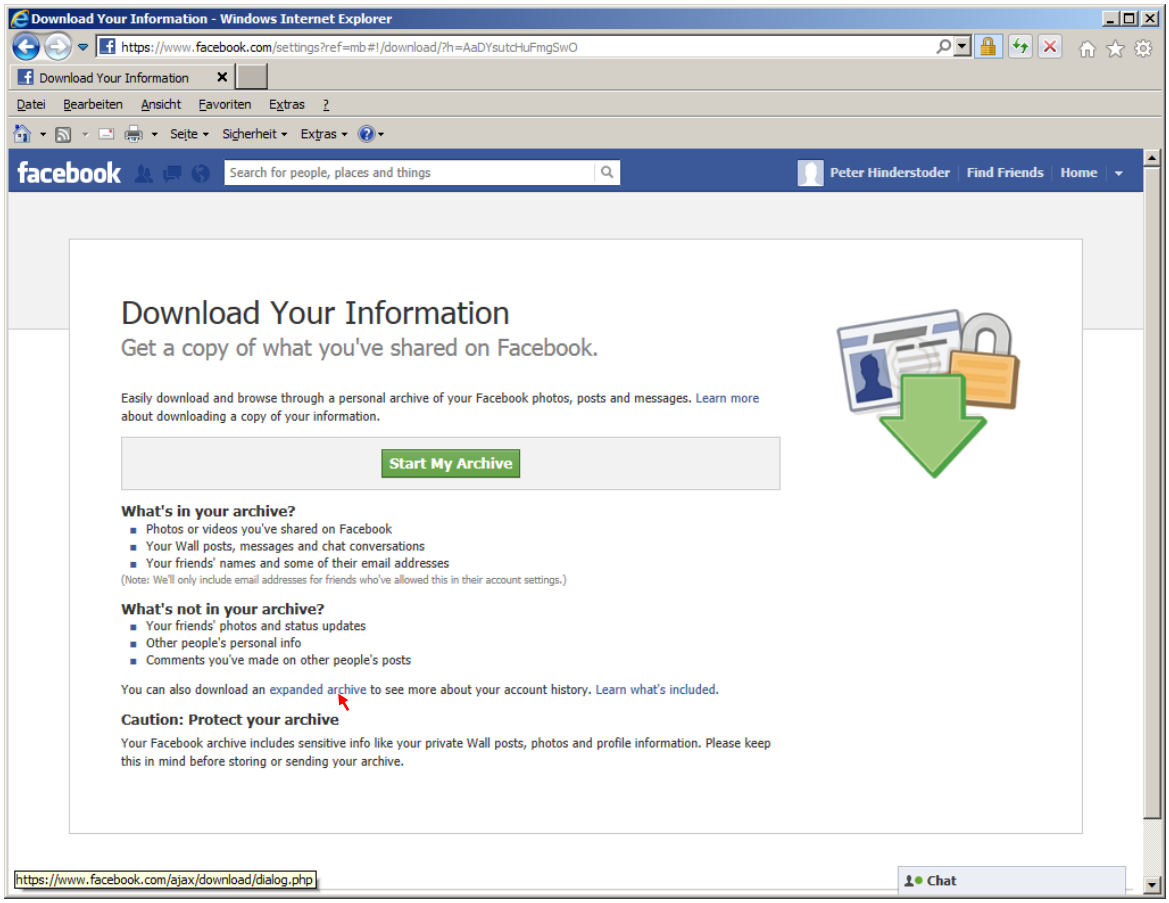
Download Tool(s) – Access

We are 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"

In addition we had to find that the "juicy" information is hidden in the "extended download tool" that can only be found when clicking on a tiny link below the main "download tool". The link is only in the 10th (!) line of text below the main tool. This separation seems 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"

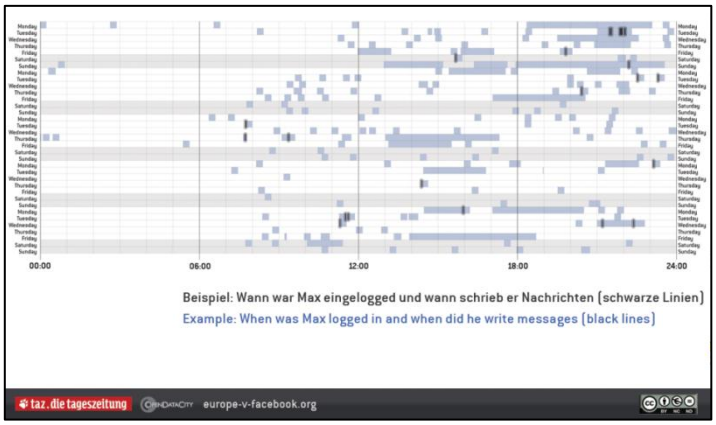
FB-I has even moved data that was previously available in the normal "download tool" to the "extended download tool". It leaves us with the impression that FB-I is ashamed of all the data it collects instead of working towards full transparency.

Especially inexperienced or older data subjects 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). We (europe-v-facebook.org) had to explain to hundreds users how to go through this in the last year!

- ➔ ***The download tools are designed to make it especially hard for users to get certain data.***
- ➔ ***There is no reasonable explanation why FB-I separates the same function into two separate tools, of which one is very well hidden.***
- ➔ ***FB-I clearly tries to fool users by making them believe that the "normal" download tool is all data it holds about them.***
- ➔ ***Even the "normal" download tool is only accessible through a tiny link.***

Download Tool(s) – Content

We have found many inconstancies when the downloaded data was compared with the "raw data" we have received previously. When comparing all three "raw" data sets with the results of today's data sets, we were missing (among other data) much of the "meta data" associated with the users' data.



Information about the user that can be derived from "meta 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".

Deleted messages, a category of data that is especially problematic (see Complaint 07), 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". We were 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.

We 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". This means that also the categories that should be displayed are obviously missing in practice.

In addition we 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. We would have never been able to uncover the misconduct by FB-I without access to the raw data sets. We therefore believe that FB-I has a vital interest not to deliver the raw data.

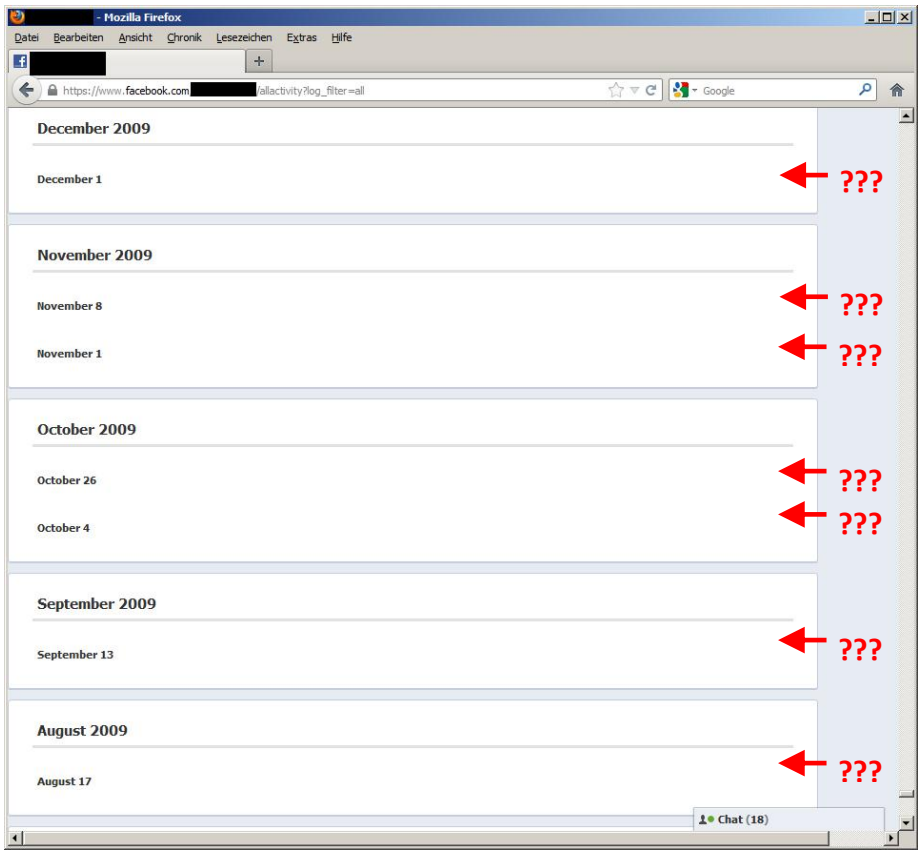
- ➔ ***The "download tool(s)" are still not delivering all data that is "personal data".***
- ➔ ***Even categories FB-I has agreed on including are not showing up in practice.***
- ➔ ***Much data is missing if compared to the "raw data" we got previously.***
- ➔ ***Deleted messages are personal data that fall under the right to access.***
- ➔ ***Given the fact that in such obvious cased like the meta data, or deleted data FB-I is not including all data, we have to reasonably suspect that other data is still undisclosed.***
- ➔ ***We ask the ODPC to explain why deleted messages are not included in the download tool.***
- ➔ ***Did the ODPD find other deleted data categories that are now not included?***
- ➔ ***We ask the ODPC to ensure that users, which are willing to pay the access fee and go through the trouble of a formal access request, get a 1:1 copy of the raw data, as it is common practice.***

Activity Log

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/EG.

The most obvious problem is, that massive amounts of data are simply missing in the "activity log". Some categories like "pages visited" are not showing up at all. Other data seems to only show up on a random basis, with declining chances the further one goes back in time: For demonstration we have collected two very obvious examples, both were taken from the account of Max Schrems on November 6th 2012.

As a very obvious sign that the "activity log" is incomplete we 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 the account of Max Schrems, there are 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) are totally missing.



Screenshot: "activity log" for the years before 2010

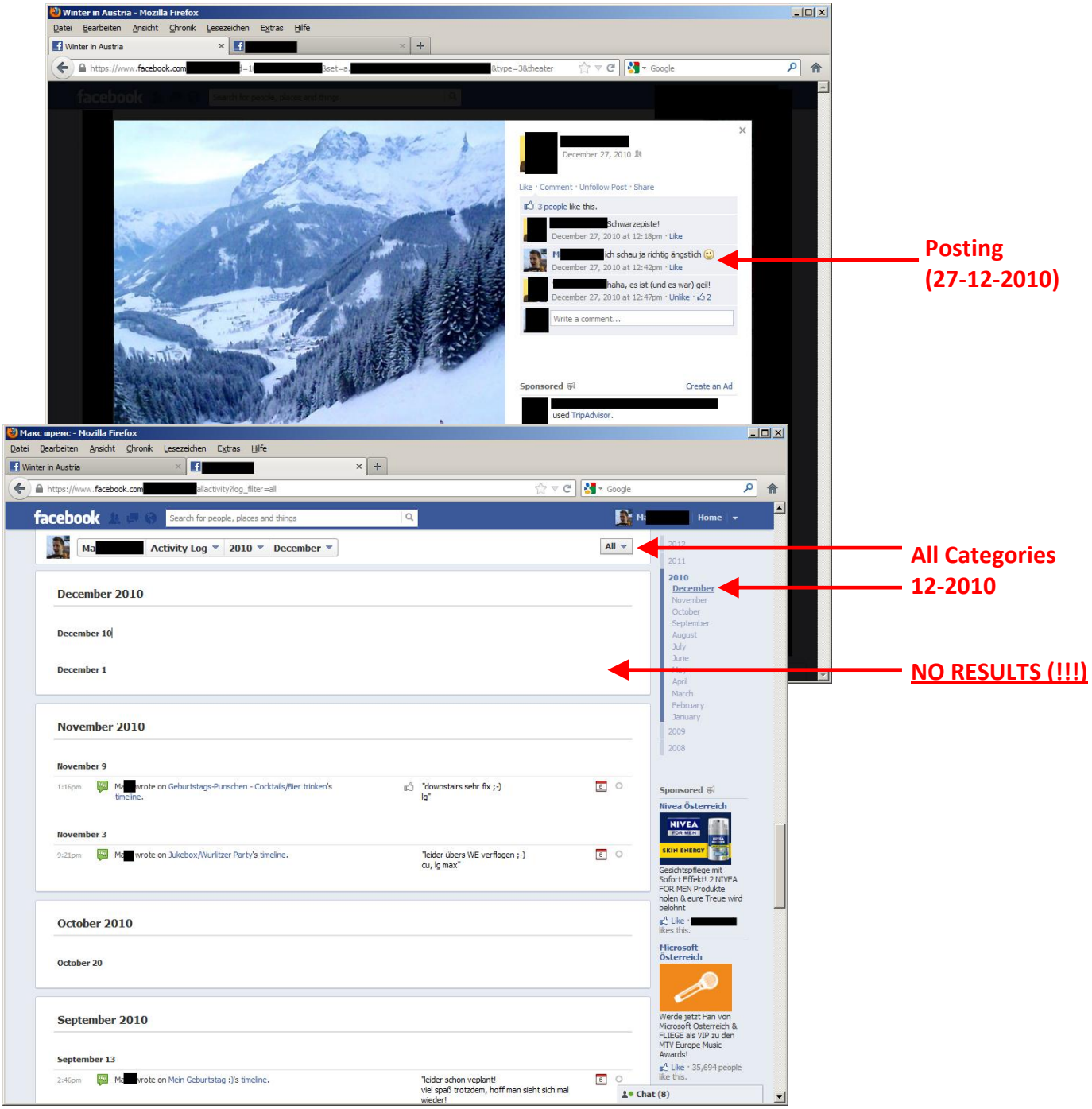
This means that FB-I does currently not give full access to the 18 data categories, despite claims that this data can be retrieved through the "activity log". The data must be stored - otherwise there should not be any "lonely dates" without any accompanying information in the "activity log".

➔ ***FB-I holds personal data but does display them in the "activity log".***

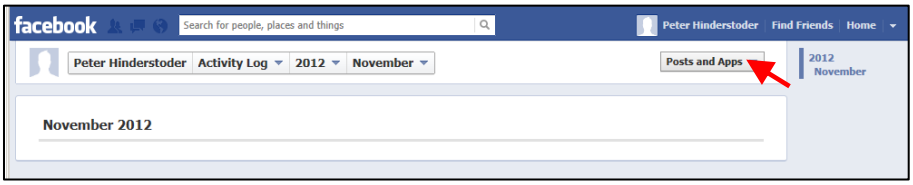
➔ ***The 18 data categories in the "activity log" are not properly made available to users.***

After we found this very obvious problem quite stunning, we have checked for more recent postings in the years after 2010. With a couple more clicks we soon discovered that also more recent data is 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 we 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,

➔ ***There was no reference whatsoever to the comment on another users' pictures, postings on other peoples pages or videos despite FB-I claiming that this data is delivered through the "activity log".***



An additional problem is that users have to click on every month of every year and then scroll up and down for minutes until the whole "activity log" is finally loaded. This procedure takes (depending on internet traffic and the speed of the users' browser) a couple of minutes to 10 minutes of constant clicking, scrolling and waiting.
Inexperienced users have no chance to get all data with a couple of clicks, since many months donot show all the data at first, but need reloading or clicking on "show more" links. The standard setting is also set to show only "posts and apps", only after changing this setting to "all", the other data is (possibly) shown. This is another obstacle for the data subjects' right to get all data.



Screenshot: Standard setting to only show "Posts and Apps"

If the data subject has finally gotten the "activity log" to load everything that's possible there is another major problem: The data is not disclosed in a tangible format.
In contrast to the "download tool(s)" there is no way of downloading the data that is contained in the activity log. Given the fact that the right to access is also a basis for other complaints this is a massive draw back. A user might only be able to take hundreds of screenshots, or print the entire page, which does in fact get corrupted when printed on a normal page. Only more experienced users will find ways to get a copy of the "activity log".

In summary FB-I does still not deliver a solid data set through the "activity log", this is 1 year and 6 months after the initial access request which was filed with FB-I on June 2nd 2011. FB-I has had more than 13 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.

In addition we have to stress, that the activity log is a form of derivative data from the raw data set, which allows for excessive manipulation or technical bugs, which in the end limit the data the users can access.

- ➔ ***FB-I received about 1.5 years since the initial requests to develop the "activity log", still FB-I is not delivering the data it is pledging to disclose through it. The tool is either full of obvious "bugs" that FB-I simply does not care about or FB-I is deliberately not disclosing all data through it.***
- ➔ ***Given the fact that in such obvious cases like demonstrated on the previous pages FB-I is not including all data, we have to reasonably suspect that other data is still undisclosed.***
- ➔ ***The data has to be delivered without obstacles in a raw format and in a tangible format.***
- ➔ ***We ask the ODPC to ensure that users, which are willing to pay the access fee and go through the trouble of a formal access request, get a 1:1 copy of the raw data, as it is common practice.***
- ➔ ***Given the extensive time FB-I was given and the poor result, we 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", "Privacy Settings" and the "Vanity URL" 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.

➔ ***It is unacceptable to send the data subjects on a "treasure hunt" all over a webpage to collect every little bit of information themselves, after going through the trouble of making a formal access request.***

Purposes, Recipient and Sources

As we 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".*

These "other users" are further specified only naming some examples: "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." *Mind:* These are only examples and *not* an exhaustive list.

In essence the "purpose" that FB-I claims is "everything we might do", not only in relation to the specific user, but also in relation to one Billion other users, companies that have a page on facebook.com, the advertisement industry, developers, other controllers and any partner.

As said before this is likely the most abstract and general purpose in the history of data protection litigation. There would be no factual difference if FB-I would simply say: *"Anything that our company does, or will do, ourselves or that might be done by anyone that we engage with."*

In direct talks with FB-I it e.g. claimed that certain data is used *"for security and other important purposes".* When we inquired about these *"other important purposes"* FB-I has told us that they cannot disclose them because of either trade secrets, or *"because you might be able to use them against FB-I".*
In this relation we want to stress, that there is no exception from the right to access that FB-I could possibly claim in order to not have to disclose the specific purpose of every operation.

The right to access is not worth the paper it is written on, if this additional information to the raw data is missing. It is impossible to determine if some form of processing personal data is allowed e.g. under Sections 2 and 2A DPA or Article 6 and 7 Directive 95/46/EG.

- ➔ ***We hereby ask the ODPC how a data subject should determine if certain personal data is still "relevant" for the purpose, only used for the specific "purpose" or obtained "fairly", if the only information that FB-I delivers is that they use the information for "other important purposes" or "in connection with the service"?***
- ➔ ***We hereby ask the ODPC to ensure that FB-I produces a fact based, all embracing description of the purposes of every category of personal data they hold about us and delivers them to us as soon as possible, since this is a crucial basis for all other complaints and therefore necessary to make our "best possible case".***

Summary – Self-Service Approach

Following what we 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 about 1.5 years, since the initial requests to respond to them. The tools are not functioning adequately.

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 afford 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. We would have never been able to file the 22 complaints without access to raw data.

- ➔ ***The ODPC has allowed FB-I to take about 1.5 years to respond to the initial access request in a correct way, instead of 40 days under the Irish DPA. This is more than 13 times (!) the legal time limit under the Irish statute, but FB-I is still not delivering the necessary data to its users.***
- ➔ ***FB-I has taken substantial efforts to deter users from getting their data, by hosting a "treasure hunt" for personal data. This results in a situation where average users are unable to get access.***
- ➔ ***The "raw data" is not delivered, much of the data is clearly missing, the tools are not properly functioning and additional information under section 10 DPA are still not disclosed.***
- ➔ ***Overall the "self-service" approach cannot substitute a traditional response to an access request and does not make FB-I complaint requests under section 10 DPA.***

D. Non-User Access Requests

As a side topic we 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 we got from non-users we have filled out this form with various information from existing non-users and with false information. No matter what we did, there was always the same result:
Even when we used e-mail addresses that have never existed, we 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.

- ➔ ***In summary FB-I is not giving a material response to access requests by non-users, but "spams" data subjects with standard 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/EG to respect the right to access by data subjects and shows FB-I's ignorance towards the rights of data subjects.***

E. Summary – Access Requests

Facebook
In summary we could hardly believe the extremely dilettantish attempt by FB-I to comply with the right to access. After 1.5 years from the initial access requests FB-I has not been delivering a full, tangible, solid and somewhat valid response to our 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/EG. It is obvious that FB-I was unable to demonstrate that we got all the data it is holding about us.

The wording of Directive 95/46/EG 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. We 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/EG.

In addition we want to mention that we have never directly gotten any e-mail or communication that would have invited us to use the new tools that were developed. The last e-mail Max Schrems 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.

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 we are aware that the ODPC does not have the necessary personal and resources to investigate every line of code, we are 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 our ability to make our case.

- ➔ ***We want to highlight that the ODPC has "waived" FB-I's duty to respond to access requests.***
- ➔ ***Even though FB-I got about 1.5 years to respond to the initial requests, which is more than 13 times (!) the legal time limit under the Irish statute the response is still not adequate.***

- ➔ ***We highlight that the ODPC is overdue to enforce our right to access as soon as possible.***
- ➔ ***We ask for a 1:1 copy of all raw data FB-I holds about us to be delivered as soon as possible. This is necessary as a basis for all other complaints.***
- ➔ ***In addition we ask the ODPC to have FB-I produce a list of all data categories and data fields FB-I processes and an explanation about the source, recipients and exact and specific purpose for all data categories.***
- ➔ ***We ask the ODPC to disclose the methodology, evidence, files and arguments in relation to the complaint concerning the right to access.***

- ➔ ***We are reassured that our initial complaint was completely justified. FB-I did clearly not deliver all personal data within the legal deadline of 40 days.***
- ➔ ***To show that a breach of the Irish law in such obvious cases is not without consequences, to prevent other companies to ignore the law as well and to show that international companies are not above the law we think that the DPC should impose a substantial penalty.***

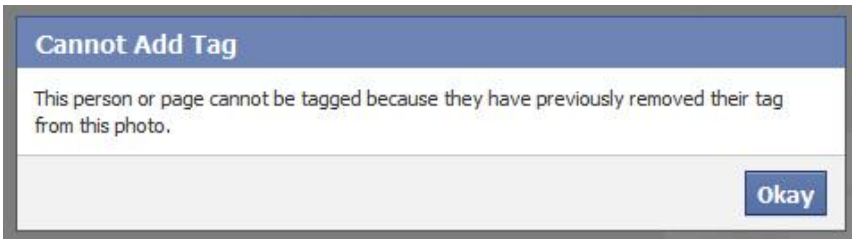
14. Complaint 11 “Deleted Tags”

Please refer to what we have brought forward above in the section on “Complaint 03 – Tags”.

Screenshot: Removing a “tag” in a posting was not working (November 7th 2012)

We want to mention that currently it seems like “removing” tags in postings does not work. We have tried to remove tags in postings in different profiles, on different computers and by using different browsers. There was only one result: Nothing happened, when clicking “remove tag”.
Therefor we were unable to assess if “removed” tags in postings are kept by FB-I. At the same time it was possible to remove tags in pictures, and we found that these tags are still kept by FB-I, without notice.

➔ ***In fact the removal of tags in postings is not working.***



Screenshot: “Removed” tag is still kept to prevent users from “retagging”

As outlined in the section on “Complaint 03 – Tags” we cannot see any major improvement, there seems to be no counterargument that we 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.

➔ ***We hereby ask the ODPC to disclose all arguments, files and evidence in relation to this complaint.***
➔ ***Currently we have no reason to believe that our initial complaint was not justified, rather we are of the view that the facts and the legal analysis were correct.***

15. Complaint 12 "Data Security"

As outlined in the initial complaint, the complaint is mainly based on the provisions of FB-I's terms. In this relation we have the feeling that the ODPC's investigation has revieled what we have suspected. The first report has made clear that FB-I was not really following "best practice" in this respect, 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."*

➔ ***From the findings in the report we are satisfied that the complaint was justified.***

At the same time we were wondering which exact methodology the ODPC and the external expert have deployed. 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."*

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."*

➔ ***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.***

This 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 hack into Facebook on CNN.

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 we 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 Max Schrems. 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) 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 form 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 one of Max Schrems: profileengine.com/#/people/10869930/max.schrems. Profiles of other members of our group show even more data publicly (see e.g. profileengine.com/#/people/17052974/andreas.kezer).

When we were searching the web for news, we soon found many other stories about scrapping and other forms of security breaches on facebook.com. Even the first report names another incident where pictures were accessible on the internet (see page 109). So overall we look at everything but a "clean record" when looking at FB-I's data security history.

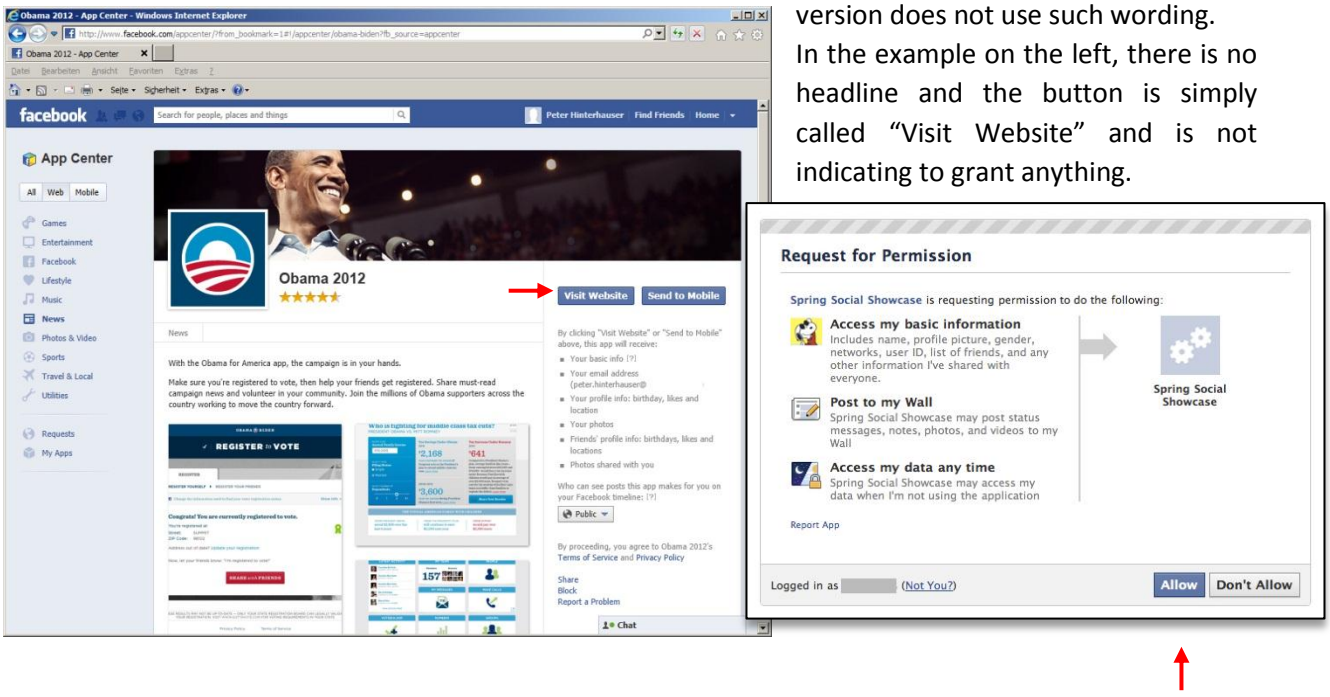
- ➔ ***There have been (widely reported) cases of successful scrapping and circumventing of FB-I's security systems.***
- ➔ ***It seems to be questionable, if only the fact that there has not been permanent coverage about data breaches and scrapping constitutes solid evidence that FB-I ensures adequate safety for users.***
- ➔ ***Therefore we ask the ODPC to disclose, as far as possible without risking the security of FB-I's operations, all evidence, arguments and files in relation to the security of facebook.com.***
- ➔ ***We also ask the ODPC to explain the methodology that was deployed to deliver the ODPC's finding in relation to FB-I's security systems.***

16. Complaint 13 “Applications”

Changes

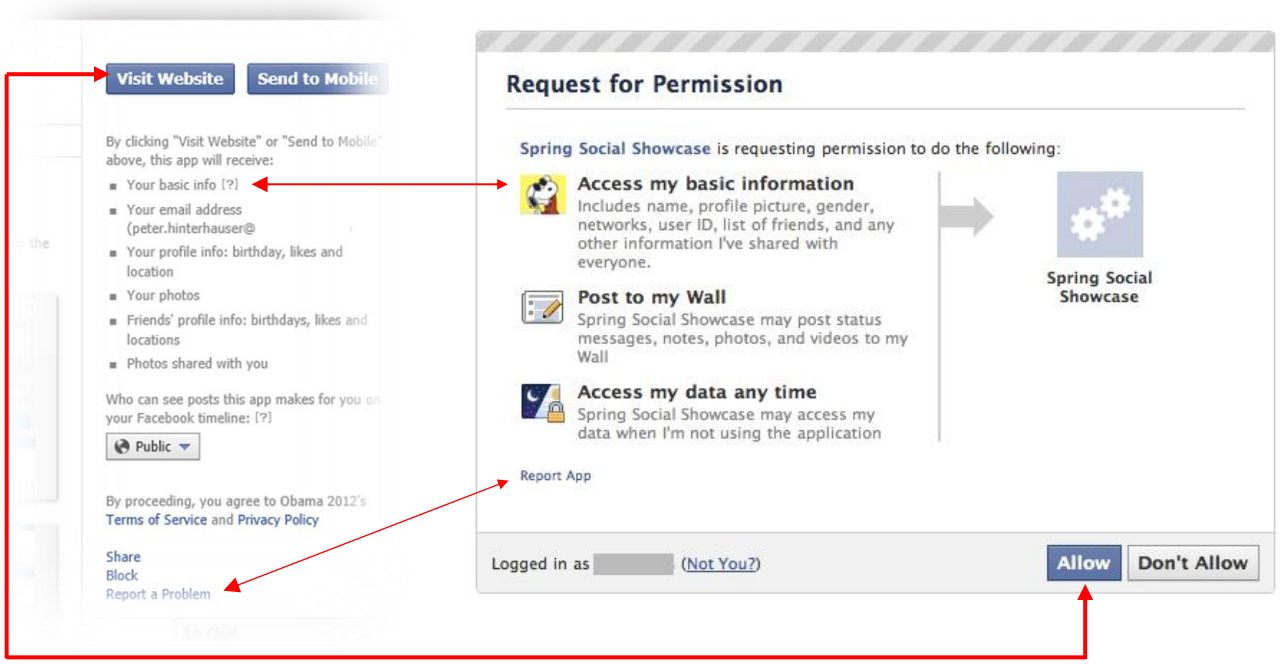
We welcomed the thorough investigation by the ODPC into third party apps, we especially thought that the insight on the possibility to “trade” tokens to be very interesting and problematic.
We want to remark that, despite the rather clear language on the side of the ODPC, there were no material changes by FB-I. The only step that seems to have derived from our 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 so this still seems to be developed from what we could read in the review. We also welcome the possibility to select the audience for posting by an app that the ODPC has pushed for.

On the other hand we 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 we 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. We 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).



Overall this is clearly a step back: The new system reminds us of the "sign up" process (see complaint 08) before FB-I improved this process. We 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, we have no reason to think that the initial complaint is not still justified.

➔ ***The new system is a step backwards and reminds us of the old sign up process.***

➔ ***We hereby ask the ODPC to get arguments about (1) why this was changed and (2) if there are statistics on how many users have aborted the process before and after the change.***

Consent by Third Parties

The main issue we 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 we are 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.

➔ ***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

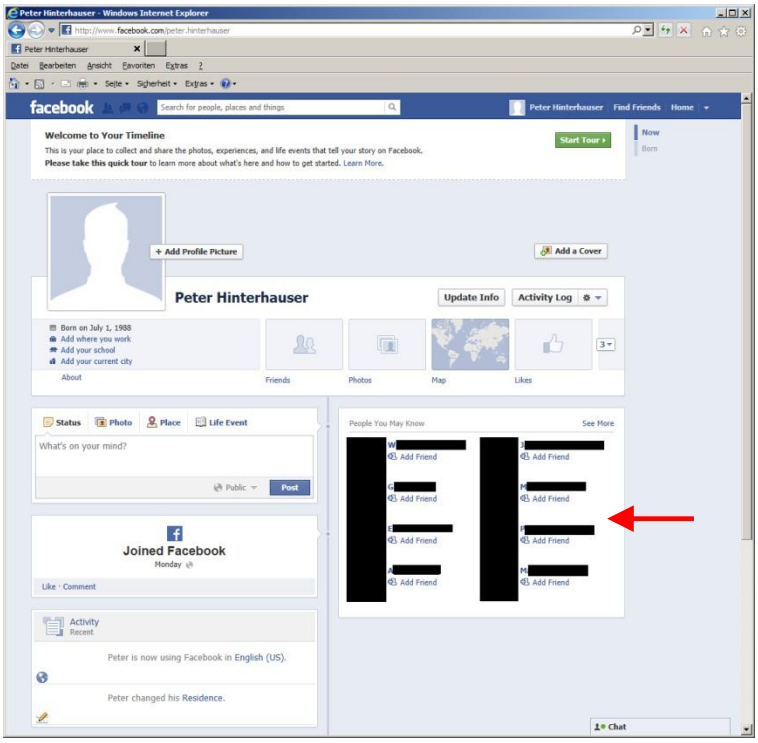
It is a core principle of Directive 95/46/EG that data must be contained in a legal sphere where the right to data protection is factually enforceable. As the ODPC has rightfully outlined in the report it is insufficient for FB-I to claim that by posting some terms on their page this would factually ensure compliance. To further develop this problem we 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 form uploading new apps or even pursuit 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.

- ➔ ***We ask the ODPC to disclose all arguments, files and evidence.***
- ➔ ***FB-I has to stop forwarding third party data to "apps" outside of a solid legal framework.***
- ➔ ***We have no reason to think that our initial complaint is not fully justified.***

17. Complaint 14 “Deleted Friends”

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.
While this small “benefit” of now suggesting removed users to be added again, this purpose does not seem to be proportionate that previous friends are kept 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.



Screenshot: Deleted friends used to promote “people you may know” (Original picture with names of the users can be delivered any time)

Independent from this question of law, we also found a new phenomenon:
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, we 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 we have opened a new profile. This profile was friends with a real user (Max Schrems). Both profiles were used to be able to make some screenshots. After this the friendship was deleted. Following the deletion FB-I was still suggesting Max Schrems’ friends to the test profile.

- ➔ ***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.***
- ➔ ***We ask the ODPC to deliver all arguments, evidence and files in relation to this complaint.***
- ➔ ***We have no reason to believe that our initial complaint would not be justified. To the contrary we think that given the fact that FB-I uses this information further they are fully correct.***

18. Complaint 15 “Excessive Processing of Data”

The reports did not analyze the exact claim in our complaint, but just 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)*

In this statement FB-I 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/EG. 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 even better results, but at some point it is excessive given the purpose of selling ads better.

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. We 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), we have to ask FB-I: 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.

- ➔ ***We ask the ODPC to disclose all arguments, files and evidence that was produced.***
- ➔ ***We currently see no reason why this complaint would not be justified, but are open for counterarguments and evidence that proof the contrary.***

19. Complaint 16 "Opt-Out"

The first part of the complaint addressed the sign up process. This has be 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.

➔ ***FB-I has changed the sign-up process towards a system that is closer to the law.***
➔ ***Therefore we understand that our complaint was justified in this respect.***

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 no substantial change by FB-I (see more details above at Complaints 08).

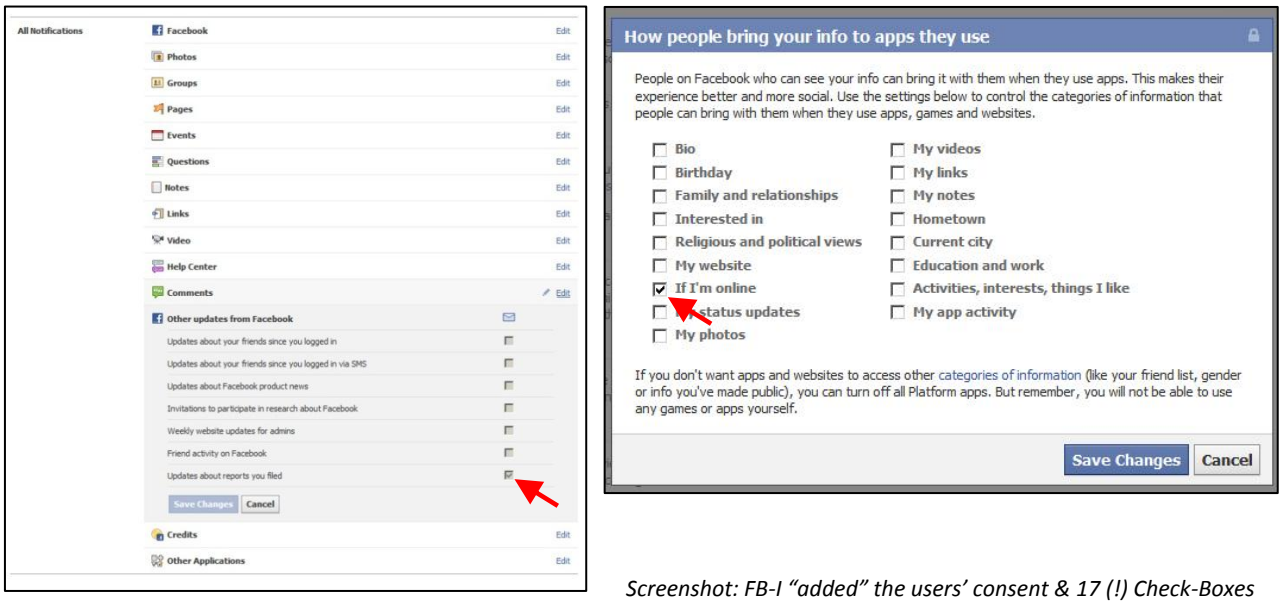
The reports did not cover the claim that FB-I deters users from choosing more privacy friendly settings, other than citing a counterclaim by FB-I that does not deliver any material arguments. It is still a long and tiring work to go through countless pages, subpages, pop-ups and deactivate one check 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 below).
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.

We 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.

- ➔ ***FB-I has not changed the default settings, even though there is a very clear interpretation of Directive 95/46/EG through WP187 and WP163 that make an "opt-out" system necessary.***
- ➔ ***The ODPC has quite clearly said that there must be substantial changes, but we cannot see them.***
- ➔ ***We hereby ask the ODPC to make FB-I produce an explanation why it only allows for "per item" manipulation of users' settings and forward this explanation to us.***
- ➔ ***We hereby ask the ODPC to disclose all evidence, arguments and files in relation to these issues and tell us if there were any other changes agreed with FB-I.***
- ➔ ***Given the view that is expressed in WP187 and WP163 and the ODPC's elaboration we have no doubt that our complaint was justified.***

In fact FB-I has even departed from the legal requirement to offer "Opt-In" function further 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 whish of the users that has unchecked all 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.



Screenshot: FB-I "added" the users' consent & 17 (!) Check-Boxes

- ➔ ***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.***
- ➔ ***We ask the ODPC to inquire about this behavior at FB-I and get back to us with the results.***

20. Complaint 17 "Like Button"

The reports have dealt excessively with social plugins and we 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 our initial complaints. We 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.

- ➔ ***FB-I does not at all contest that is 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.***
- ➔ ***It has yet to be checked if also non-users can be tracked in a personal way (e.g. by connecting the browser cookie with a person). We ask the ODPC to investigate on this or disclose all information that would clarify this question.***

Purpose

After repeatedly reading all documents from the ODPC we 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).
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."
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 we have to assume that the audit failed to list all purposes FB-I uses the data for. In addition the "security" argument was also deployed in a letter sent to us by Richard Allen, which would constitute another purpose not listed in the two reports.
A limitation of purposes is also not reflected in the privacy policy of FB-I: 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."*

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, we 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 we 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 of FB-I 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 "motorbikes", "Harley Davidson" and "Cisco". If there would be a 1:1 relation, such difference would 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.

Overall we 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 we were given by FB-I.

- ➔ ***While there might be a factual limitation of the purposes which FB-I uses the data for, it is allowing itself to use such information for any purpose under its policy.***
- ➔ ***There is so far no solid 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.***
- ➔ ***We ask the ODPC to get a list of all operations that are done using "social plugin" data.***
- ➔ ***We ask the ODPC to disclose all evidence, arguments and files that were produced in relation to this issue.***

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 (we 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 we have submitted in the initial complaint that make the form of processing illegitimate. We 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.

- ➔ ***We ask the ODPC to disclose all evidence, arguments and files that were produced in relation to this issue and ask the ODCP to get the other necessary facts and counterarguments from FB-I.***
- ➔ ***Currently we have no reason to believe that our initial complaints were not justified, especially given the fact that the ODPC has forced FB-I to make multiple changes.***

21. Complaint 18 “Obligations as a Processor”

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 we have pointed out. There is also no statement form FB-I that we could find in the reports.

➔ ***We ask the ODPC to produce and disclose relevant files, arguments and evidence.***
➔ ***Currently we have no doubt that our initial complaint was and is justified.***

22. Complaint 19 “Picture Privacy Settings”

The report and the technical analysis did not bring forward any new facts or arguments that were not already known in the initial complaints. Our 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 our 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.

➔ ***We ask the ODPC to produce or disclose files and arguments in relation to this complaint.***
➔ ***We currently have no doubt that our initial complains were justified.***

23. Complaint 20 “Deleted Pictures”

We 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 we were 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.

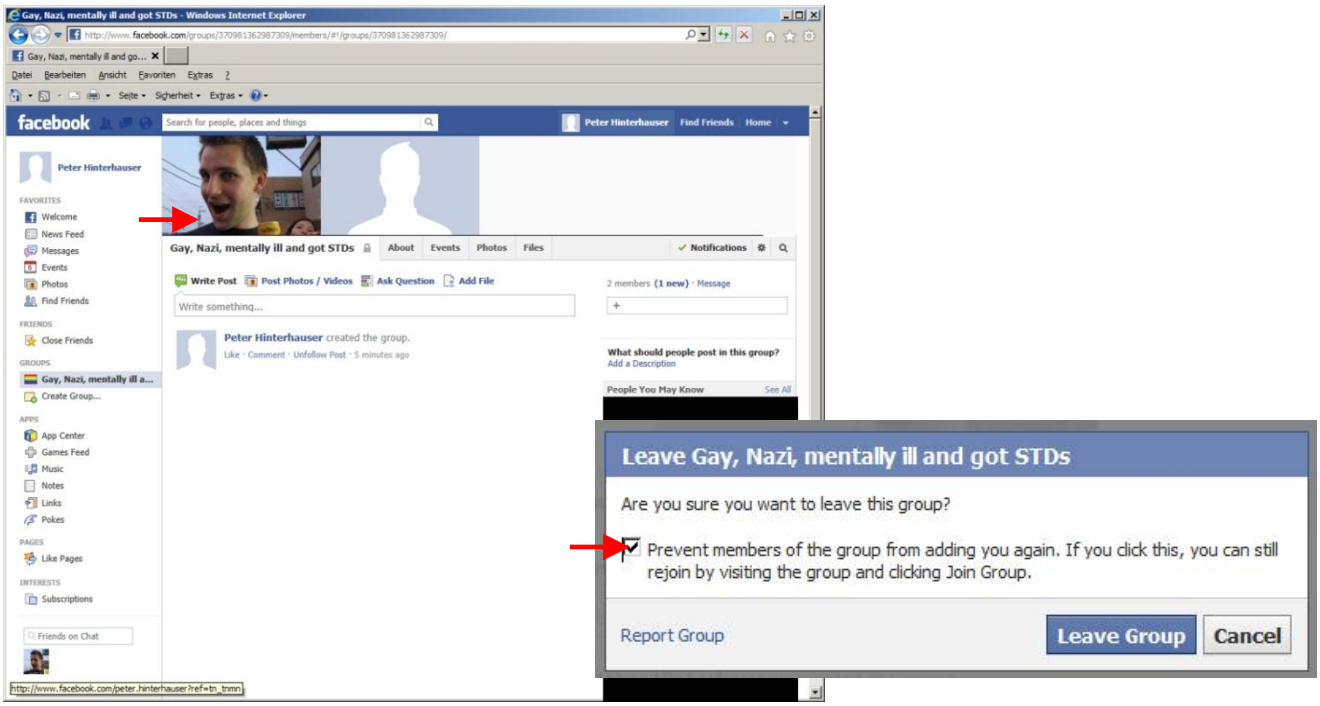
➔ ***We were unable to see any material change.***
➔ ***We ask the ODPC to disclose any documents that would allow us to assess FB-I’s response.***

The report has not at all covered the issue that Akamai is a US company, but not on the Safe Harbor. We have not received any arguments, evidence or files that indicate that the use of an external processor was covered under the law.

➔ ***We ask the ODPC to produce or disclose such evidence, as well as any other files, evidence or arguments in relation to this complaint.***
➔ ***Given the facts above, we have no doubt that our initial complains were justified.***

24. Complaint 21 “Groups”

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 (we named some in our screenshot below).



Screenshots: Users that were invited to the group “Gay, Nazi, mentally ill and got STDs”

When users have left a group, then 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 we have outlined at “Complaint 02 – Tags” that also works for “groups”.

- ➔ ***FB-I has made some (little) steps in the right direction which indicates that our initial complaints were justified, which we 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.***
- ➔ ***We cannot see any reason why the invitation to “Groups” is treated any different from “events” or “pages” that need a clear affirmative action by the data subject.***
- ➔ ***We ask the ODPC to disclose any substantive counterarguments by FB-I.***

25. Complaint 22 “New Policy”

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. We understand that this agreement from November 29th 2011 was meant: http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf

This agreement has nothing to do with our 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 automatically covering foreign subsidiaries that do not even cater to US consumers.

- ➔ ***We ask the ODPC to deliver FB-I’s response to the complaint, so that we can assess if the complaint is still justified.***
- ➔ ***We ask the ODPC to disclose all evidence, arguments and files that refer to this issue.***

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.

FB-I has previously pointed at its great option for users to even vote on any change of privacy policies when more than 7.000 users demand it. When our group has tested this pledge, by getting about 45.000 people to ask FB-I to make certain changes, it has conducted a vote, but was hiding it in such a way that just 0,038% of its worldwide users have voted. The turnout of 86,9% against the vote was simply ignored.

To our understanding FB-I has not even managed to conduct the change in the privacy policy under its very own provisions, which can only be read in a way that a “real” vote has to be conducted. But it can be even less in line with the law, to simply change the essence of what users have given their unambiguous, informed and specific consent to. This would totally undermine the essence of the “informed consent” in the law.

- ➔ ***Currently we have no doubt that our initial complaint was and is justified.***