To the
Data Protection Commissioner
Canal House, Station Road
Portarlington , Co. Laois
IRELAND

Maximilian Schrems
[redacted]
[redacted]
AUSTRIA

Vienna, June 25th 2013

Complaint against Facebook Ireland Ltd – 23 "PRISM"

To whom it may concern,

This is a formal complaint against "Facebook Ireland Ltd" under section 10 of the Irish DPA and at the same time also a request for a formal decision by the DPC. There is probable cause that "Facebook Ireland Ltd" is breaking the Irish DPA and the underlying Directive 94/46/EG and I kindly ask you to investigate the following complaint, inform me about your findings and make a legally binding decision after a conducting fair trial.

Facts of the Case:

I have been a user of "facebook.com" since 2008. Facebook stores large amounts of data about me (see previous – so far undecided – 22 complaints). My user ID is "[redacted]", but my account is also visible under my name and registered to my emai[redacted]. The Facebook service is provided to users outside of the USA and Canada by "Facebook Ireland Ltd" who is in my view partly a controller and partly a processor of my data (see other complaints filed in 2011). "Facebook Ireland Ltd" is not processing the data itself but transfers the data of its users to the USA where it is factually processed by "Facebook Inc".

"Facebook Inc" is subject to the "EU-USA Safe Harbor" system under which the users' data is transferred to the USA. There is no compulsory reason to transfer my personal data to the USA unless it is e.g. communicated to users in the USA. In general my data could also be held within the EU/EEA. "Facebook Ireland Ltd" seems to be using the services of "Facebook Inc" as a (sub-)processor voluntarily or only for economic reasons.

The British Guardian newspaper has now published documents by the US National Security Agency (NSA) that show that "Facebook Inc" is forwarding its user data to the NSA for reasons of espionage, national security and other matters. Facebook is listed in these documents as granting "mass access" to such data without any need for a probable cause since June 3rd 2009 under a program called "PRISM". The published documents indicate that "Facebook Inc" is participating (among other companies) in the PRISM program voluntarily. Other companies that provide similar services (like e.g. twitter) are not listed in the documents published by the Guardian. In addition, services were added over time, which is also pointing at a voluntary cooperation.

There are substantial reasons to assume that the facts revealed by the Guardian are correct. The involved companies have unanimously denied the direct access to its servers or even the knowledge of a program called PRISM. They only refer to numbers and laws that allow access to individual pieces of information in their statements. At the same time there was no such claim by the heads of the administration of the United States. If the reports were in essence false, one would have expected a quick and clear denial by the heads of the US government, but in fact the reactions have not at all been denying the allegations.

The first reactions by President Obama (http://on.wsj.com/14FU8eB) and the Director of National Intelligence James Clapper (http://tinyurl.com/lltzz5g, http://tinyurl.com/mmos4fd and http://tinyurl.com/mwgu9d6) have not clearly denied direct access to the servers of "Facebook Inc" and the other companies involved. President Obama has explained details about access to communication data of "Verizon" but has not given any details on the accusations by the Guardian concerning the PRISM program. In different statements by James Clapper the NSA has further explained the rights to access under § 1881a U.S.C. While there are some clear words on the rights of US citizens, I was unable to find any clear statement that would deny access to or mass collection of data from non-US citizens. If the reports by the Guardian would be essentially wrong or if the published documents would not be genuine, it would have been logical to clearly and unambiguously reject the reports.

The companies involved are, according to their own statements, bound to secrecy under US laws ("gag orders"). This means that they are not allowed to say the truth about any such processing and are even bound to lie about such a program. Given this legal regime, the public statements by "Facebook Inc" are neither credible nor a reason to question the reports by the Guardian. So far neither "Facebook Inc" nor "Facebook Ireland Ltd" have issued a statement under an obligation to tell the truth or disclosed evidence that would prove the non-existence of the described cooperation with the NSA.

The statement that the NSA cannot "directly" access the servers of "Facebook Inc" reminds me very much of the facts in the "SWIFT" case. In this case the US government has installed a "black box" which was used to get full access to the financial transaction data stored by "SWIFT". The US government has thereby gained access to data in a way that is effectively equal to a direct access of servers.

- ➔ ***Summarizing the above: It is clear that "Facebook Ireland Ltd" is the controller or processor of my data. "Facebook Ireland Ltd" has outsourced the processing of my data to "Facebook Inc" and is therefore transferring my data to servers in the USA.***
- ➔ ***There is probable cause to believe that "Facebook Inc" is granting the NSA mass access to its servers that goes beyond merely individual requests based on probable cause.***
- ➔ ***The statements by "Facebook Inc" are in light of the US laws not credible, because "Facebook Inc" is bound by so-called "gag orders".***

- ➔ ***Therefore I ask the DPC to further clarify the facts and consult "Facebook Ireland Ltd" if they can prove by any means that the reports by the Guardian are false or substantially inaccurate.***
- ➔ ***As with all previous complaints against "Facebook Ireland Ltd", I understand that I will receive the outcome of such a clarification in line with my rights under Art 6 ECHR and the Irish law.***
- ➔ ***If there are any reasons to withhold such documents I hereby ask the DPC to limit such a restriction of my right to access to files to the minimum necessary and explain the reasons for a denial of access.***

Legal Arguments:

Controller:
To my understanding "Facebook Ireland Ltd" is the controller and/or processor of my data. This is also reflected by the terms of use on "facebook.com". "Facebook Inc" is correspondingly the processor or sub-processor that handles the data on behalf of "Facebook Ireland Ltd". Therefore "Facebook Ireland Ltd" is subject to the Irish Data Protection Act (DPA) and Directive 95/46/EC.

Purpose Limitation:
In Work Paper (WP) 128 on the Belgian financial services provider "SWIFT" the Article 29 Working Group has held that the mass use of *commercial* data for *investigative purposes* is a breach of the principle of purpose limitation. This argument equally applies to the data held by "Facebook Ireland Ltd" if such data is further used in masses for purposes like "terror prevention" or espionage. Therefore such usage by "Facebook Ireland Ltd" or its (sub-)processors is in breach of Article 6(1)(b) of Directive 95/46/EC and Section 2(1)(c)(ii) of the DPA.

As the Article 29 Working Group has already found in WP 128 the ECJ has interpreted Article 6 of the Directive 95/46/EC in light of Article 8 ECHR and has held that the forwarding and use for another purpose is interfering with the right to privacy under Article 8 ECHR and can therefore only be legitimate if it is "necessary in a democratic society" (see decisions C-465/00, C-138/01 and C-139/01 by the ECJ).

Proportionality:
In WP 128 the Article 29 Working party has said: *"The Working Party points out that even for the purposes of alleged terrorism investigations only specific and individualized data should be transferred by SWIFT on a case by case basis, in full compliance with data protection principles. As this is not the case, the current practice is not proportionate and thereby violates Article 6 (1) (c) of the Directive."*

Since the facts of the case are equivalent if now "Facebook Ireland Ltd" is (via "Facebook Inc") forwarding user data to the NSA in bulk it seems clear that the processing operations by "Facebook Ireland Ltd" are equally in breach of the DPA and Article 6(1) of Directive 95/46/EG.

Interpretation in line with WP 128: In the case of "SWIFT" the Article 29 Working Party has also considered the fact that the data was transferred to the US voluntarily: *"As a result by having decided to mirror all data processing activities in an operating center in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law and where a processing of personal data has been organized in a way that appears to circumvent the structures and international agreements already in place."*

This argument must equally apply in the case of "Facebook Ireland Ltd". Because of its onward transfer of data to the US, "Facebook Ireland Ltd" has put itself in an equally foreseeable position in which the mass access of the NSA via its parent company "Facebook Inc" was even possible. Therefore "Facebook Ireland Ltd" cannot justify the situation with US regulations, if the arguments from the "SWIFT" decision are applied.

Transfer of Data to the US:
As mentioned above my data is processed in the US by "Facebook Inc". This means that thereby "Facebook Ireland Ltd" is transferring my data to a third country without an "adequate level of protection". Correspondingly Article 25 of Directive 95/26/EG and section 11 DPA apply to such transfers. A transfer to a third country without an adequate level or protection is only allowed under Article 25 of Directive 95/46/ if the fundamental rights and the right to data protection of the data subjects enjoy adequate factual and legal protecting in the third country.

The exceptions under section 11(4) DPA clearly do not apply. "Facebook Ireland Ltd" might argue that users have consented to such transfer, but users have surely not given an *informed* consented to the processing of their personal data in the US. "Facebook Ireland Ltd" has not informed its users about mass access and about

the cooperation with the NSA. To the contrary, "Facebook Inc" and "Facebook Ireland Ltd" is denying any such cooperation. Therefore there cannot be any informed consent.

As I know of no other basis that would make the transfer to the US legal under section 11 of the DPA or Directive 95/46/EG, I am further assuming that the transfer from "Apple Ireland" to "Apple Inc" is only done under the "Safe Harbor" system.

Safe Harbor:
"Facebook Inc" has joined the "Safe Harbor" (http://safeharbor.export.gov/companyinfo.aspx?id=18810) and has thereby self-certified that that it adheres to certain data protection principles (e.g. concerning the onward transfer of data). As far as I know the transfer of data to "Facebook Inc" is done solely on this legal basis.

Members of the "Safe Harbor" have pledged to limit onward transfer of data to third parties. In particular they have to adhere to the principles of "notice" and "choice". This means that there needs to be consent and proper information to data subjects if data is transferred. Both principles were not followed if user data was forwarded to the NSA in bulk. Concerning third party data stored on Facebook accounts, there is no practical possibility to adhere to such "choice" and "notice" principles.

Exception for "national security": Under the fourth paragraph of annex 1 of the "Safe Harbor" decision the adherence to the principles of the "Safe Harbor" can be limited for purposes of "national security".
I am therefore asking the DPC to inquire if "Facebook Inc" is forwarding my data to the NSA for compelling reasons of national security or if merely cooperating with the NSA voluntarily.
I further ask the DPC to inquire if this onward transfer of data to the NSA is in line with the exceptions from the "Safe Harbor" or if such an onward transfer is exceeding the exception and is therefore illegal. I kindly ask the DPC to consider the arguments below concerning the interpretation of this exception.

Exception for "statutory law": Under the fourth paragraph of annex 1 of the "Safe Harbor" decision the adherence to the principles of the "Safe Harbor" can be limited to comply with laws or even case law. According to the reports by the Guardian the mass access to the servers of "Facebook Inc" is bases on § 1881a U.S.C. (also known as 702 FISA).
I am therefore asking the DPC to inquire if Facebook's forwarding of my data to the NSA is necessary for compliance with § 1881a U.S.C. or if "Facebook Inc" is merely cooperating with the NSA voluntarily.
I further ask the DPC to inquire if this onward transfer of data to the NSA is in line with the exceptions from the "Safe Harbor" or if such an onward transfer is exceeding the exception and is therefore illegal. I kindly ask the DPC to consider the arguments below concerning the interpretation of this exception.

Interpretation of the "Safe Harbor" Decision:
The mere wording of the European Commission's Decision on the adequacy of the "Safe Harbor" from July 26th 2000 (L 2000/215, 7) could be interpreted in a way that the above mentioned exceptions would in reality be a "wildcard" that would allow the US to limit the application of the "Safe Harbor" decision by the European Commission as it pleases. Equally any form of data gathering for "national security" would be blankly exempt. In addition there is no definition or limitation of this "national security" exception. The exceptions under letter "a)" do also not include any limitation that would allow balancing these exceptions with the fundamental rights of data subjects.

If one would follow this interpretation, any form of onward mass transfer of personal data from an American processor to US authorities would be totally legal under EU law. Such mass surveillance would also be legal without any reasonable suspicion, without judicial overview and without any adherence to the fundamental rights equal to the ECHR and the CFR. Such an interpretation of the "Safe Harbor" could in no way be in line with Article 25 of Directive 95/46/EC, would be against recital 10 of the Directive 95/46/EC and would be in breach of Article 8 ECHR and Article 8 CFR.

But if the "Safe Harbor" decision is viewed within the hierarchy of the legal system, it seems clear that it is necessary to consider higher ranking fundamental rights and the directive when interpreting a decision of the European Commission. Otherwise one would imply that the European Commission's decision itself is not in line with these higher ranking laws.

Narrow interpretation in line with Directive 95/46/EC:
The "Safe Harbor" decision must be interpreted in line with Directive 95/46/EC, because the decision by the Commission cannot exceed the boundaries of the underlying law.

This means that when interpreting the exceptions above, it may only be interpreted in a way that the "adequacy" of the level of protection is in line with Article 25 of Directive 95/46/EG and in line with WP 12 of the Article 29 WP. Otherwise one would assume that the Commission has passed a decision that is in breach of Directive 95/46/EC. This possibility if covered below.

The adequacy of the protection of personal data does not only concern private use of data but also includes the public access and handling of such data, as the Article 29 WP has already pointed out in WP12 concerning contractual clauses: *"Article 6 of the Amsterdam Treaty also guarantees respect for the fundamental rights set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms. In third countries similar limitations on the ability of the state to require the provision of personal data from companies (…) may not always be in place. (…) In some cases a contract is too frail an instrument to offer adequate data protection safeguards, and transfers to certain countries should not be authorised."*

In particular the DPC should investigate if a blanket exception for "national security" or "statutory law" of the US can be in line with Directive 95/46/EC and the users' fundamental rights under the European Union treaties. Until today it was primarily held that only the "national security" and laws of EU member states – and not any third country – can create exceptions for data processing. Otherwise the DPC would have to clarify in which case the "national security" or the law of a foreign country can be used to waive EU data protection laws.

If processing and a transfer of EU data for "national security" or the "laws" of third countries would be in line with Directive 95/46/EG this would also allow for a blanked transfer of data to any other foreign government (like Russia, China, Iran or North Korea) which can be in no way in line with EU legislation and the ECHR.

Narrow interpretation in line with Article 8 ECHR and Article 8 CFR:
The Irish DPA and Directive 95/46/EC have to be interpreted in line with the fundamental rights under the ECHR. This is not only derived from general legal principles but was also ruled by the ECJ (see e.g. § 21 of the ECJ's decision C-465/00, C-138/01 and C-139/01 of May 20th 2003). After the coming into force of the Lisbon treaty this must consequently also apply to the Charta of Fundamental Rights of the European Union (CFR).

An interference with the fundamental right to privacy can only be allowed under the ECHR if it is necessary in a democratic society and has to be additionally "proportionate" under the CFR. A mass transfer of European users' data to a foreign authority without any reasonable suspicion and with no effective legal remedy for the data subjects can in no way be in line with the fundamental rights we enjoy under the ECHR and the CFR. A mass access to content data without an individual justification and without individual judicial oversight cannot be in line with the fundamental rights we enjoy in the European Union. Consequently Directive 95/46/EC must be interpreted in a way that does not allow for such mass access.

In addition it would be highly questionable when the rights that are guaranteed under Article 8 ECHR and Article 8 CFR could be bypassed by forwarding EU data to third countries without such guarantees. Just like the principle of "non-refoulement" in asylum cases it has to be clear that a transfer of data to a third country that does not adhere to our understanding of fundamental rights would undermine our fundamental rights.

This issue becomes especially obvious if the results from the PRISM project are shared with European intelligence authorities as it was reported in many member states. In the end this would result in an "outsourcing" of government surveillance to territories outside of the scope of the ECHR and CFR. In contrast, my understanding is that the ECHR and the CFR require the EU and the member states to actively protect my fundamental rights – also against foreign countries.

➔ ***I am therefor asking the DPC to ensure that the "Safe Harbor" Decision is interpreted in line with Directive 95/46/EG and fundamental rights. If it is necessary we recommend getting a preliminary ruling by the ECJ.***

Validity of the "Safe Harbor" Decision?

If the DPC is unable to interpret the "Safe Harbor" decision in line with Directive 95/46/EC, the ECHR and the CFR, the logical consequence would be that the decision by the European Commission is invalid. It is clear that the European Commission can only form a decision within the boundaries of such higher ranking laws.

The "Safe Harbor" decision was repeatedly and massively criticized, because there are reasons to believe that it does not guarantee an adequate level of data protection as described under Article 25 of Directive 95/46/EC. Until now the main point of criticism was the protection from companies in the US and what was frequently perceived as limited possibilities of enforcement. But Article 25 of the Directive 95/46/EC does not only cover the protection from private parties but covers a much broader scope of "adequacy" of the protection of fundamental rights (see references above). This also includes the protection from public authorities in a third country on a legal and factual level. This much broader scope must be observed when deciding about the "adequacy" of a transfer to a third country.

The initial adequacy decision by the European Commission on the "Safe harbor" from the year 2000 is especially problematic because of the massive changes in US legislation after the terror attacks of 9/11. Following these terrorist attacks the US have introduced many new laws and factual practices that hardly comply with European ideas of fundamental rights and the rule of law.

EU citizens are generally exempt from constitutional protection of their fundamental rights, since the US is still following the idea of "civil rights" (only applying to US citizens and people inside of the US) instead of "human rights". A "mass confiscation" of the EU citizens' data is therefore not covered by protections under the US constitution, but instead expressly allowed under § 1881a U.S.C. (also known as 702 FISA). There is no effective judicial oversight, because only the service provider – not the data subjects – can take legal action. The relevant FISA court forms its decisions behind closed doors and it has been reported that it has so far almost never refused any requested access to data. In addition, many other laws like the "Patriot Act" allow access to the data of European citizens in a way that is hardly in line with European fundamental rights. A more detailed elaboration on this matter is outside of the scope of this first submission on this matter.

While the adequacy decision by the European Commission might have been within the limits of Directive 95/46/EC when it was delivered in 2000, there are now serious doubts if the US is still giving "adequate" protection to the fundamental rights of European citizens on a legal and factual level. Therefore I have serious reason to believe that the adequacy decision by the European Commission might become subsequently invalid because of changes in the US legal system, as well as changes in the factual protection of EU nationals' privacy.

➔ ***I am therefor asking the DPC to review the validity of the "Safe Harbor" decision and if necessary get a preliminary ruling by the ECJ on this matter, given the pan-European importance.***

Burden of Proof when transferring data to third countries:
Following the wording of Article 26(2) of Directive 95/46/EC and the systematic view on section 11 DPA the controller has the burden of proof for an adequate level of protection in a third country. This means that "Facebook Ireland Ltd" has to clarify and encounter my data is processed by "Facebook Inc" in a way that legally and factually ensures an adequate protection of my fundamental rights. This is also true within the "Safe Harbor" Framework (see e.g. decision by the German "Düsseldorfer Kreis" on April 28th/29th 2010).

If "Facebook Ireland Ltd" would refuse further clarification with reference to a "gag order" under US law, the only logical consequence would be that the transfer of personal data to "Facebook Inc" would need to be prohibited, because "Facebook Ireland Ltd" would not be able to demonstrate adequate safeguards in line with Article 26 of Directive 95/46/EG. This would clearly mean that a transfer to the US would be illegal.

- ➔ ***In summary it is clear that a "mass access" to personal data without a reasonable and specific suspicion against an individual is illegal under the ECHR and the CFR.***
- ➔ ***Such mass access would be in breach of the principle of "purpose limitation" as defined in Article 6(1)(b) of Directive 95/46/EC and Section 2(1)(c)(ii) of the DPA.***
- ➔ ***Such a wide access to personal data would further be illegal under the principle of proportionality under Article 6(1) of Directive 95/46/EG and the DPA.***
- ➔ ***In addition Directive 95/46/EC allows a transfer of personal data to a third country only if an "adequate level of protection" is guaranteed which is at least equal to the protection under the ECHR and the CFR.***
- ➔ ***A bulk transfer of personal data to the NSA would therefore be in breach of section 11 DPA and Articles 25 and 26 of Directive 95/46/EC as well as the ECHR and the CFR.***
- ➔ ***According to section 11 DPA and Article 26(2) of Directive 95/46/EC the controller has to ensure that adequate protections of the users' fundamental rights are in place. It is therefore upon "Facebook Ireland Ltd" to prove that the reported forwarding of data is not actually happening. If "Facebook Ireland Ltd" is unable to provide solid proof, any transfer to "Facebook Inc" in the US would need to be stopped.***

- ➔ ***I am therefor asking the DPC to investigate this complaint and if necessary stop the transfer of data to "Facebook Inc", if "Facebook Ireland Ltd" cannot prove that the reported forwarding of data to the NSA is not taking place.***

Thank you for protecting the fundamental rights of European citizens. I am available for further questions via [redacted] as well as via phone at [redacted] This complaint is digitally signed and therefore a legally binding complaint. Please note that similar complaints were and will be filed concerning other companies involved in the PRISM scandal in Ireland and other member states.

Kind Regards,

Maximilian Schrems