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

Mag. Maximilian Schrems
[redacted]
[redacted]
AUSTRIA

Vienna, December 1st 2015

**Complaint against Facebook Ireland Ltd**

To whom it may concern,

This is an update to my initial complaint against "Facebook Ireland Ltd" dated 25th June 2013. All facts and submissions are made supplemental to my complaint dated 25th June 2013. Please refer to the initial complaint in relation to all matters not dealt with in this update.

As a preliminary point, my solicitors wrote to Facebook Ireland Limited on 12th October 2015 requesting details of all legal basis that they were relying on to transfer my data to the US. Furthermore, I requested a copy of any contract that they purported to rely on. Unfortunately, Facebook Ireland Ltd has only responded to my request on Friday, 27th November 2015 at the end of the business day. The response from Facebook Ireland Limited's solicitors attached an Agreement dated 20th November 2015 between "Facebook Ireland Ltd" and "Facebook Inc". The request to identify any other legal basis for transfers between Ireland and the United States of America has not been comprehensively answered by "Facebook Ireland Ltd". Instead, they state "*In addition to the Agreement, Facebook Ireland relies on a number of additional legal means to transfer user data to the US*".

I am sure your office very much welcomes that the following comprehensive "update" to my initial complaint is submitted within two business days, despite the fact that "Facebook Ireland Ltd" has taken 6 weeks to furnish my solicitor with a simple copy of their SCCs. Therefore, given the above, the criticism leveled by your office against me in relation to your suggestion that I was "delaying" "updating" my compliant do not stand up to scrutiny.

# A. FACTS

## 1. "Facebook Ireland Ltd" transfers my personal data to the United States

"Facebook Ireland Ltd" forwards my personal data to "Facebook Inc." in the United States of America, where my data is processed. Facebook Ireland Ltd is subject to the Irish DPA and consequently Directive 95/46/EC. Both seem to be undisputed by "Facebook Ireland Ltd".

## 2. "Facebook Inc" is subject to US surveillance laws

"Facebook Inc" is subject to a number of known and secret laws, rules, court decisions and executive orders that oblige it to make my personal data available and/or oblige it to disclose it to US authorities, such as e.g. the National Security Agency (NSA) and the Federal Bureau of Investigations (FBI). These laws include e.g. 50 U.S.C. § 1881a that apply to any "electronic communication provider" and require it to turn over any "foreign intelligence information", or rules like Executive Order 12.333 among others.

My personal data, as well as, for example, all information in relation to my dealings with your office, fulfills the definition of "foreign intelligence information" (e.g. because of my actions in this and other procedures that are relevant for the US government).

But even if my data would not fall under this definition, US law targets data – not individual people. This means that as long as "Facebook Inc" holds any relevant information on its systems, it has to make all data available to the US government, independent of the relevance of each piece of information and the person it relates to. In other words: US law, like, for example, § 1881a applies to all data that an "electronic communication provider" holds, not to the data of each personal "target". Accordingly US access is based on "certifications" and "directives" that are not aimed at an individual person, but aimed at certain "data pools".

As US law does not target people, but data – there is also no judicial remedy that would allow the data subject to take appropriate action. Non-US persons are also not covered by constitutional protections in the US. The relevant "United States Foreign Intelligence Surveillance Court" operates in full secrecy, on an *ex parte* basis. The judges are appointed solely by the US government. It has only denied 12 of more than 35,000 requests since 1979. This "court" basically amounts to a "rubber stamp" operation that may have the word "court" in its name, but misses almost all elements of a "court" in practice. In summary "court" does not fulfill any requirement of a "court" in a "democratic society" (Art 6 ECHR and/or Art 47 CFR).

The fact that "Facebook Inc" is subject to these laws is also admitted by "Facebook Inc" in their letter from 8th July 2013, where they highlight "*significant constraints*" under US surveillance laws to disclose any facts on the relevant programs. This argument already contains the confession that "Facebook Inc" is subject to the relevant laws.

## 3. "Facebook Inc" is subject to "gag orders"

"Facebook Inc" is subject to "gag orders" that orders it to deny and/or not disclose any facts about these surveillance systems. Only specific persons, who have the necessary clearance, are allowed to know about the relevant systems.

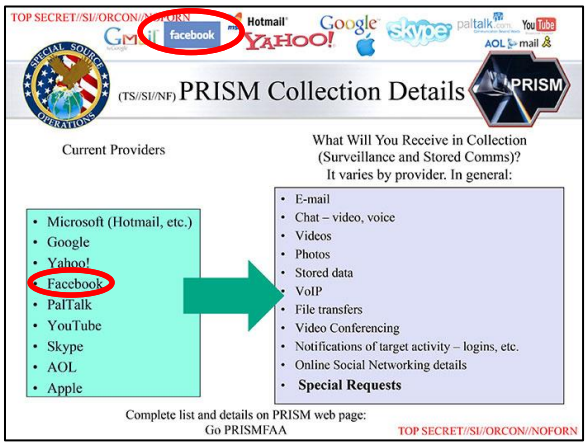
It is obvious to anyone aware of this situation, that any comment or assurance from "Facebook Inc" must be reviewed in the light of these legal circumstances. Even high ranking company officials may not even hold the necessary clearance to know what is done within their own company. A statement by an entity or person that is obliged to lie under its domestic law has absolutely no value, given that such statements do not lead to any liability and that any comment that confirms the facts would lead to serious consequences under US law.

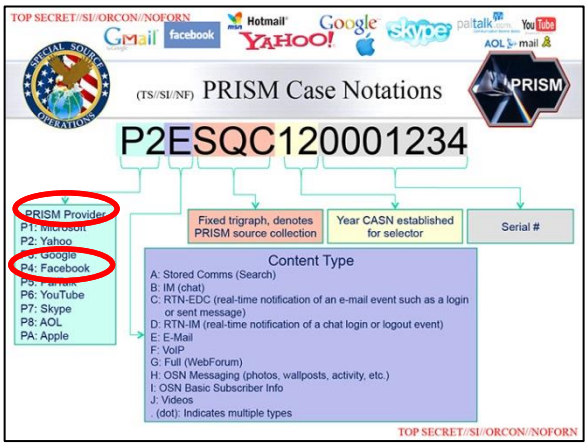
This problem extends to US officials, lawyers and representatives of "Facebook Inc", and especially "Facebook Ireland Ltd" that will typically either not be in possession of the relevant information and/or be "bound to lie" under US law.

The fact that these orders are regularly used is not only known from a number of disclosures and leaked court orders that were issued by US courts under 50 USC Chapter 36 (see e.g. leaked FISA court order from April 25th 2013[1]), but also admitted in the letter from 8th July 2013 by "Facebook Inc", where they highlight "*significant constraints*" under US law.

## 4. "Facebook Inc" factually complies with US surveillance laws

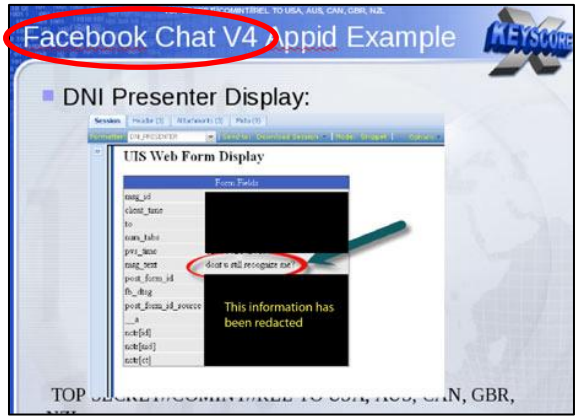
The disclosures by Edward Snowden have proven that "Facebook Inc" (among other internet companies) are not only subject to US law in abstract, but also factually participating in US mass surveillance systems like "PRISM" and "XKeyscore" to name only two of many. The relevant documents are surely known to the DPC and are publicly available. As mere examples I would like to submit the following "slides" which (as many others also do) directly refers to Facebook and the data collected from facebook.com:

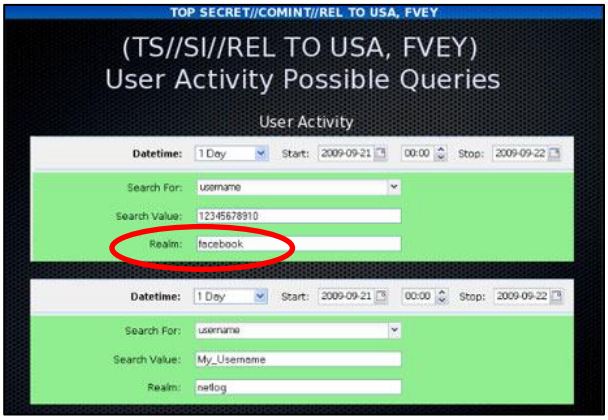



[1] *Full title of the order: "IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM VERIZON BUSINESS NETWORK SERVICES, INC. ON BEHALF OF MCI COMMUNICATION SERVICES, INC. D/B/A VERIZON BUSINESS SERVICES."*

The "slides" make it clear, that Facebook Inc is not just a minor data source that grants individual access to user data, but one of the nine main sources ("PRISM Provider") with its own ID ("P4") and fully participates in the program. Equally, Facebook is explicitly named in the XKeyscore documents that show how US government officials can "search" Facebook data.




This fact seems to be only disputed by "Facebook Inc". Not any other entity of relevance (e.g. the European Commission, the European Parliament, the European Court of Justice, the EDPS, the Article-29-WP, all national member states that were parties to the procedure before the CJEU, the Irish High Court, the investigations and reports by the US "Privacy and Civil Liberties Oversight Board" or the US government itself) disputed these facts.

As your office is surely aware of all the relevant documents, working papers and submissions referred to above, I would spare us to repeat them, highlight that the US government itself(the only entity – other than certain persons within "Facebook Inc" – who have first-hand information of the factual situation) repeatedly confirmed these facts. As an example:

> "*The federal government has been secretly collecting information on foreigners overseas for nearly six years from the nation's largest Internet companies like Google, Facebook and, most recently, Apple, in search of national security threats, the director of national intelligence confirmed Thursday night.*" http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html

The only dispute between the US and European governments seem to be that the massive access, availability and/or collection of data is not seen as "*mass surveillance*" under the US constitution by the US government, but clearly constitutes an interference with Art 7 and 8 CFR and Art 8 ECHR. However this is clearly a legal question – not a factual question (see clarification by the CJEU and further details below). The fact that there is factual access to Facebook data under PRISM is general consensus.

In line with these findings the DPC has taken the only reasonable view, which is that the US government does use US internet companies to conduct different forms of "mass surveillance". This was confirmed by your office in a number of public statements, such as e.g. the interview on RTÉ radio with Commissioner Billy Hawkes on June 10th 2013 where Mr Hawkes confirmed that he doesn't "*think that it will come as much of a surprise that in fact US intelligence services have access to information from US companies*".

## 5. "Facebook Ireland Ltd" relies on denials by "Facebook Inc"

As said before, "Facebook Inc" has not produced any credible assurance in light of the acknowledgements and finding of the US government, the European and Irish courts and governments and the documents released by Edward Snowden.

The documents recently released by your office, in which "Facebook Inc" reassures "Facebook Ireland Ltd" that data controlled by "Facebook Ireland Ltd" is not subject to US mass surveillance are at least deeply troubling, if not embarrassing.

In fact the letter of "Facebook Inc" sent to "Facebook Ireland Ltd" on 8th July 2013 is simply a copy/paste exercise of the following press statements by "Facebook Inc":

A blog post by Mark Zuckerberg (available at https://www.facebook.com/zuck/posts/10100828955847631), numbers about government access that *do not* cover the relevant legal basis (https://govtrequests.facebook.com/country/United%20States/2014-H2) and finally a general press release by "Facebook Inc" (http://newsroom.fb.com/ news/2013/06/facebook-releases-data-including-all-national-security-requests/). In summary "Facebook Ireland Ltd" was obviously fed the same generic "PR speech" that everyone in the world could read on Facebook's web pages. It is therefore also unclear to me why this compilation of public statements in the form of a letter should be "confidential" in the view of your office.

The letters do not, by any means, address the specific allegation, the application of the relevant law and the practices. It does not explain how the Snowden "slides" and confirmations by the US government add up with the total denial of "Facebook Inc". If these slides are not genuine it would, for example, beg the question why the United States is engaged in a global man hunt for Edward Snowden and the UK government sent government agents to *The Guardian* newspaper to destroy the IT systems the data was stored on.

To the contrary "Facebook Inc" has explicitly stated that "*the law imposes significant constraints on the ability of companies like Facebook to even confirm or acknowledge receipt of national security requests*". This clearly acknowledges that "Facebook Inc" cannot fully and freely confirm the factual extent of US mass surveillance of personal data transferred by "Facebook Ireland Ltd".

In summary "Facebook Inc" basically states "*I can't talk about this – but trust me everything is fine*" in a situation where every evidence and action by the relevant players proves the opposite.

It was extremely unreasonable for "Facebook Ireland Ltd" to rely on a letter that is a copy/paste collection of press statement, accompanied with the clear acknowledgement that the sender cannot freely speak about the relevant facts.

## 6. Findings of the Irish High Court

The findings of the Irish High Court in *Schrems -v- Data Protection Commissioner*, which are binding case-law in this respect, were very explicit on the factual side of the case. To just repeat some findings starting at paragraph 4 of the judgement:

> *"4. While it is true that the Snowden disclosures caused – and are still causing – a sensation, only the naïve or the credulous could really have been greatly surprised."*

*"5. Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed – or, if you prefer, has had cast upon it – far-reaching global security responsibilities."*

*"13. While there may be some dispute regarding the scope and extent of some of these programmes, it would nonetheless appear from the extensive exhibits contained in the affidavits filed in these proceedings that the accuracy of much of the Snowden revelations does not appear to be in dispute. The denials from official sources, such as they have been, were feeble and largely formulaic, often couched in carefully crafted and suitably ambiguous language designed to avoid giving diplomatic offence. I will therefore proceed on the basis that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion."*

## 7. Factual personal Consequences

Even if this is not relevant under the law and only for the sake of completeness, I would like to submit that [redacted]

## 8. "Facebook Ireland Ltd" does not identify other legal grounds for a data transfer

My solicitors wrote to Facebook Ireland Limited on 12th October 2015 and requested the following:

*„Therefore, we require you to identify, by close of business on Friday 16th October 2015, all legal basis that you are relying to transfer our client's data to the US. When replying, we call upon you to forward us a copy of any contract relied on by you."*

In their reply dated 27th November 2015 "Facebook Ireland Ltd" has refused to identify all legal bases that it uses to transfer data to the United States. This fact is especially relevant given the duties to inform data subjects (actively, but at least upon request) about these grounds under the law. The fact that "Facebook Ireland Ltd" has refused such information upon request may render any of these grounds invalid in any event.

## 9. Summary

In summary, there is clear evidence that leads me to believe that my personal data, controlled by "Facebook Ireland Ltd", and processed by "Facebook Inc", is at the very least "made available" to US government authorities under various known and unknown legal provisions and spy programs such as the "PRISM" program. There is also a reasonable likelihood that my personal data has, in addition, also been accessed under these provisions.

# B. LEGAL ANALYSIS

## 1. Definition of "Processing"

Most arguments by "Facebook Inc" and "Facebook Ireland Ltd", as well as the US government, centre on the actual form of data processing by the US government.

While some claim that the US government actually "*stores*" all relevant information in huge data centres (currently in Utah), and, as admitted in the case of "Verizon" forwarding data to a government storage system similar to the EU's data retention (see leaked FISA court order from April 25th 2013), others claim that providers (such as "Facebook Inc") allow "access" to all personal data stored on their servers, while only a small fraction of the data is actually transferred to and stored by the US government.

While these differences may be relevant under US law, all of these arguments are in fact irrelevant under EU law. Article 2(b) of Directive 95/46/EC defines "*making available*" as a form of "processing". So even if my personal data is never "*accessed"* by any US government agency, the mere fact that "Facebook Inc" has to make this data "*available*" (for example,. under 50 U.S.C., Chapter 36) triggers not only Directive 95/46/EC, but also Art 8 CFR that uses the same definition of "processing" as Article 2(b) of Directive 95/46/EC.

While I explicitly maintain that I have every good reason to believe that my personal data stored on the systems of "Facebook Inc" was and is in fact "*accessed"*, I would like to highlight that only the fact that certain data must be "*made available*" seems relevant for an assessment of US law and practices in the light of EU fundamental rights and Directive 95/46/EC and the Irish DPA.

Finally, I would like to reiterate that this complaint is actually concerned with the illegal transfer and/or disclosure of my personal data from "Facebook Ireland Ltd" to "Facebook Inc" which constitutes the relevant processing operation under Directive 95/46/EC and the DPA, in the light of the facts set out above. The operation of the "mass surveillance" systems in the United States is therefore only a secondary matter that has to be taken into account when assessing the legality of the relevant processing operation – which is the transfer from "Facebook Ireland Ltd" to "Facebook Inc". Both operations are separate under the law and are not to be confused.

## 2. Charta of Fundamental Rights (CFR)

As the CJEU has found in the judgement C-362/14, mass and indiscriminate surveillance, such as under the PRISM program is not just "disproportionate", but is also a violation of the "essence " of the Right to Respect for my Private Life under Art 7 CFR (see para 94 of the judgement). The CJEU also found a violation of the essence of the Right to Effective Judicial Protection under Art 47 CFR (see para 95 of the judgement) in the case of US mass surveillance.

The CJEU judgment makes it clear that already on the basis of the CFR the actions "Facebook Inc" is involved in cannot – no matter which kind of secondary law or decision "Facebook Ireland Ltd" may claim – be legal under primary EU law.

Under the continuous case law of the CJEU, any form of secondary legislation (such as Directive 95/46/EC or any Commission Decision and the relevant implementation in the member states' law, as in this case the Irish Data Protection Act) must be interpreted in the light of the CFR and in the clear interpretation of the CJEU in this particular case.

## 3. Irish Constitutional Law

Similar results can be derived from Irish constitutional law, as *Hogan J.* has held:

> *"53. Such a state of affairs – with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker - would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41)."*

Obviously the Irish Data Protection Act has to be interpreted not only in the light of EU law (mainly the CFR and Directive 95/46/EC) but also in the light of the Irish constitution. The High Court judgment makes it clear that already on the basis of the Irish Constitution the actions "Facebook Inc" is involved in cannot – no matter which kind of national law or decision "Facebook Ireland Ltd" may claim – be legal under the Irish constitution.

## 4. General Remarks on Transfer to a Third Country under Directive 95/46/EC

Articles 25 and 26 of Directive 95/46/EC (as implemented in Section 11 of the Irish DPA) generally prohibits transfers of personal data outside of the EEA unless the third countries that were found to provide adequate protection.

The United States of America has never provided such "adequate protection" as a country. After the judgement C-362/14 even US companies that have self-certified under "Safe Harbor" do not provide such an adequate protection. Transfers to the US are therefore generally prohibited.

"Facebook Ireland Ltd" continues to transfer my personal data (just like the data of all other Facebook users) to "Facebook Inc" in the United States. Under the law, it is therefore the duty of "Facebook Ireland Ltd" to guarantee and prove that all personal data that is transferred to a third country is adequately protected in that third country. If in doubt, the transfer of data to the United Stated must be prohibited.

Directive 95/46/EC is also based on an abstract assessment of the protection in a third country, as it is typically impossible to review the factual protection in foreign countries.

Under the law, I therefore only have to prove that my data is transferred to a country that does generally not provide adequate protection. I do not have to prove that my data is in fact "made available" to US authorities (which it is) or even accessed by US authorities (which it is). The law also does not require establishing any kind of "secondary harm" or direct consequence from the transfer (which would render the law basically unenforceable), as the CJEU has clarified in C-362/14.

In other words: It is (a) not upon me to prove that my data is transferred to a country where it is not adequately protected, but upon "Facebook Ireland Ltd" to prove the opposite and (b) the assessment is to be taken from an abstract (legal) perspective and only in a second step by reviewing the factual compliance with the law.

"Facebook Ireland Ltd" is obviously unable to succeed on any of these levels.

## 5. Specific Justifications under Directive 95/46/EC

In the letter of 27th November 2015, "Facebook Ireland Ltd" has denied any comment on the method(s) used to transfer data to the United States other than an "Agreement" based on Decision 2010/87/EU and "*a number of other additional legal means*" that they apparently intend to address "*as part of the now ongoing … investigation*".

Given this clearly defensive and unhelpful response by "Facebook Ireland Ltd" I am unfortunately not in a position to make any final comment on the legal basis "Facebook Ireland Ltd" may argue in the course of these proceedings, which could have led to a fast decision. However, there are a number of options "Facebook Ireland Ltd" will likely try to argue. In the interest of a swift procedure I would therefore comment on the following options in advance:

### a. Standard Contractual Clauses

According to the letter from 27th November 2015, "Facebook Ireland Ltd" claims to rely on "Standard Contractual Clauses", in the version of Commission Decisions 2010/87/EU.

### (1) Validity of the arrangement provided

**Application of SCCs significantly limited by undisclosed additional agreements**

The clauses used by "Facebook Ireland Ltd" and "Facebook Inc" significantly differ from the ANNEX to Decision 2010/87/EU, most notably:

- The contract provided is giving priority to some blacked out arrangement named in Clause 2.3 over the ANNEX to Decision 2010/87/EU. Unless this legal basis is disclosed, "Facebook Ireland Ltd" cannot possibly rely on Decision 2010/87/EU if the ANNEX is altered in a way that it is overruled by some non-disclosed element.
- The contract provided gives priority to "*other intragroup agreements in the Facebook group*" over the ANNEX to Decision 2010/87/EU. Unless these agreements are disclosed, "Facebook Ireland Ltd" cannot possibly rely on Decision 2010/87/EU if the ANNEX is altered in a way that it is overruled by some non-disclosed "intragroup agreements".

As Commission Decision 2010/87/EU only applies to "*standard contractual clauses set out the Annex*" according to Article 1 of the Decision, "Facebook Ireland Ltd" cannot claim the benefits of Decision 2010/87/EU when using an altered contract that allows other undisclosed elements to overrule the agreement. The nature of "Standard Contractual Clauses" is that a controller cannot

independently overrule these standards. Accordingly Clause 10 of the ANNEX to Decision 2010/87/EU states that:

> *"The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause."*

Amazingly, this Clause 10 was even copy/pasted by "Facebook Ireland Ltd" to its alternative agreement, even if the clauses clearly contradicts the amendments made by "Facebook Ireland Ltd", as they explicitly limit the application of the Clauses in the ANNEX to Decision 2010/87/EU.

**Contracts covering Sub-Processors missing**

As known to your office, "Facebook Ireland Ltd" and/or "Facebook Inc" use a large number of sub-processors to provide its services (for example Akamai as a CDN). The relevant contracts have to be disclosed under Clause 4(h) of the Agreement, which "Facebook Ireland Ltd" has failed to do. It is therefore not possible to assess the legal protection of my personal data if my data is processed by the various sub-processors.

**Type of SCCs used does not cover all processing operations**

In addition it seems that "Facebook Ireland Ltd" has simply used the wrong decision to cover all data transfers. From everything known "Facebook Inc" does not only process data as a "processor" but also uses the same data as a "controller" when providing services to its own users (namely all Facebook users living in the United States and Canada). These processing operations are subject to the SCCs in Decision 2001/497/EC or Decision 2004/915/EC.

Under the alternative agreement provided by "Facebook Ireland Ltd" it seems as "Facebook Inc" is clearly *not* allowed to use data as a controller. Therefore "Facebook Ireland Ltd" would have to ensure that "Facebook Inc" does only use the relevant personal data as a "processor" not a "controller" and request "Facebook Inc" to suspend all processing operations as a "controller".

**Signatures missing and/or wrong**

While surely more of a formalistic matter, "Facebook Ireland Ltd" has chosen to blacken the signatures of the contracting partners. It is the most relevant element of a contract, that it is signed by an individual that is capable of binding the relevant companies. Clause 4(h) of the Agreement allows "commercial information" to be redacted, but this would clearly not apply to the signature of the agreement itself, which does not constitute "commercial information".

Interestingly the Annexes 1 und 2 to the agreement are even signed the wrong way: "Facebook Inc" is signing as the "data exporter" and "Facebook Ireland Ltd" as the "data importer". Unless the flow of data reverses at times the contracting parties were not even able to find the right spot to put their names and company seals, which begs the question about the seriousness of the whole exercise overall.

Given that "Facebook Ireland Ltd" is very keen to require the even most absurd formalistic evidence in this procedure (as well as in the ongoing civil procedure in Vienna) I cannot accept that the very same entity does not even provide the a copy of the most relevant element of any contract, namely the signatures in a case where the relevant contracting partners seem to be even unable to sign in right spot. "Facebook Ireland Ltd" is therefore unable to prove that the alternative agreement presented by it is even effective.

**Previous Agreements not disclosed**

For the complaint (which covered the time from the first use of "facebook.com" in 2008 or at the latest the date where "Facebook Ireland Ltd" has taken over my contract from "Facebook Inc") "Facebook Ireland Ltd" cannot only rely on the most recent arrangement that was entered into last week. "Facebook Ireland Ltd" did not provide any legal basis for the past 7 years.

**Summary on the Validity of the SCCs used**

In summary, "Facebook Ireland Ltd" cannot possibly rely on Decision 2010/87/EU on the basis that it does not even fulfill the most basic formal requirements: It does not cover all processing operations by "Facebook Inc", it does not include the necessary arrangements with sub-processors, it is not even signed in a verifiable way and obviously only applies to transfers within the last week.

Most notably "Facebook Ireland Ltd" has chosen to depart from the text in the ANNEX to the decision. Accordingly, the DPC is not at all "bound" (let alone "absolutely bound") by Decision 2010/87/EU, Article 26(4) of Directive 95/46/EC and/or 11(2) of the Irish Data Protection Act. At the same time the DPC *is* bound by the judgments of the CJEU in C-362/14 and the High Court in *Schrems -v- the Data Protection Commissioner* and the CFR as well as the Irish Constitution, which clearly prohibit a transfer in this situation, as set out above.

"Facebook Ireland Ltd" has not proven that the alternative agreement was authorized by the DPC under Section 10(4)(ix) DPA. Even if it would be, such an authorization would be invalid and void in the light of the judgements C-362/14 and *Schrems -v- the Data Protection Commissioner* and therefore irrelevant in this procedure.

## (2) Exception to Decision 2010/87/EU (and all other SCCs)

Even if the current and all previous agreements between "Facebook Ireland Ltd" and "Facebook Inc" would not suffer from the countless formal insufficiencies above and would be binding for the DPC (which it is not), "Facebook Ireland Ltd" could still not rely on them in the given situation of factual "mass surveillance" and applicable US laws that violate Art 7, 8 and 47 of the CFR (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held).

Article 4(1) of Decision 2010/87/EU (as all other relevant Decisions) takes account of a situation where national laws of a third country override these clauses, and allows DPAs to suspend data flows in these situations:

*"(1) … competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:*

*(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;"*

This section is taken from Art 4(1)(a) of Decision 2010/87/EU, but all other decisions that "Facebook Ireland Ltd" may claim in these procedures have similar exceptions. The fact that the "PRISM program" violates the *essence* of Art 7 and 47 CFR was clearly established by the CJEU and is binding on the DPC. Art 13 of Directive 95/46/EG that the Commission Decisions refer to has to be interpreted in the light of Art 7 and 47 CFR. The question if US surveillance laws go beyond the level allowed under Art 13 of Directive 95/46/EC was clearly established by the CJEU through its judgement in C-362/14.

The exception also requires that there is a likely adverse effect on the guarantees provided by the law and the SCCs. In this respect I would like to highlight that the law does not require a factual harm, but an adverse effect on the legal protection by the clauses, which is clearly given in this case.

In short: Merely the fact that "Facebook Inc" is subject to the relevant US law as set out above (independent from the evidence that "Facebook Inc" actually complies with them), if read in the light of the CFR and the Irish Constitution, render data flows from "Facebook Ireland Ltd" to "Facebook Inc" illegal.

In addition, the factual processing operations by "Facebook Inc" and the fact that "Facebook Inc" has not even informed "Facebook Ireland Ltd" about the access by US authorities, would constitute (among other things) a violation of the Clauses and would trigger a suspension of data flows under Article 4(1)(b) and (c) of Decision 2010/87/EU as well.

In summary the DPC can invoke the exceptions of Article 4(1) of Decision 2010/87/EU (even if it would be bound by the Decision itself) to give full effect to the fundamental and constitutional rights violated by the transfer, as held by the CJEU and the Irish High Court.

### b. Consent

It is very much disputed that the rights under Art 7 and 47 CFR can be "waived" through consent. In addition "consent" to be freely given requires that a user has the free choice between different options. Given that "Facebook Ireland Ltd" has basically become a utility and users cannot choose between having their data transferred to the United States or not, the user is not in any situation that would allow for a "freely given consent". I therefore submit that consent is *not* a legal basis for any data usage that violates fundamental rights under Art 7, 8 and 47 CFR.

Even if fundamental rights under the CFR can be "waived" in these cases, consent under Art 8 CFR and Article 26(1)(a) of Directive 95/46/EC has to be (1) freely given, (2) specific, (3) informed and (4) unambiguous in relation "*to* the *proposed transfer*".

"Facebook Ireland Ltd" currently informs users that data is "*data is transferred outside of the EEA*" in its privacy policy. This is the only wording "Facebook Ireland Ltd" uses that can be even remotely be debated as constituting "consent", even if this is only information.

The wording does that does not even remotely refer to the United States or the relevant fact that his data is subject to "mass surveillance" or certain US laws. The claim in the privacy policy of "Facebook Ireland Ltd" also lacks any form of precision to ever be "specific" or "unambiguous" as required under the law. Basically "Facebook Ireland Ltd" only says that data may be transferred "*anywhere* in the whole wide world".

Consent under this provision is clearly not "*informed*" in relation to the relevant facts (which includes that the transferred data is shared with the US government on a mass scale) as "Facebook Ireland Ltd" maintains that the data processed by "Facebook Inc" is *not* made available to the US government. A controller that aggressively claims that a certain processing operation does *not* take place can hardly argue that he "*informed*" data subjects that exactly this specific processing operation is taking place.

Consequently this information does not fulfill any of the four requirements for consent, as a user should be (a) informed in a specific and unambiguous way about the relevant facts (including that all personal data on facebook.com is made available to US agencies as a form of mass surveillance) and (b) be "freely given". In fact this wording is maybe the most ambiguous, *un*specific form of (mis)information that "Facebook Ireland Ltd" could possibly use.

Facebook as a group of undertakings is obviously trapped between EU law requiring proper information by "Facebook Ireland Ltd" and US "gag orders" prohibiting such information to be provided by "Facebook Inc", which is why legally binding "consent" seems to be impossible in this situation.

### c. Any other legal basis

Any other derogation under Article 26(1) of Directive 95/46/EC that "Facebook Ireland Ltd" may argue must again fail on the basis that the CJEU has been very clear that transfers that lead to the use of such data for "mass surveillance" are a violation of Art 7, 8 and 47 CFR.

As Directive 95/46/EG and the Irish Data Protection Act have to be interpreted in the light of the CFR and/or the Irish Constitution it is clearly a logical and legal impossibility to justify a transfer that violates these constitutional and fundamental rights under national laws or secondary EU legislation. There is clearly no legal option for "Facebook Ireland Ltd" to circumvent the CJEU and the High Court judgments under the Irish constitution and/or the CFR without violating the Irish constitution and/or EU fundamental rights.

For the avoidance of doubt I would still like to submit that the derogations in Article 26(1)(b) to (e) of Directive 95/46/EC and the relevant subparagraphs of Section 11 of the Irish DPA that apply if a transfer is "*necessary*" cannot apply in this case, as it is clear from the statements by "Facebook Ireland Ltd" that they merely "outsource" data to "Facebook Inc". This transfer is very

likely a processing operation that is of great financial and practical value to "Facebook Ireland Ltd" but not "*necessary*" by any means. "Facebook Ireland Ltd" could, for example, process the personal data it holds as a controller in data centres within the EEA and (if it wishes to link its systems with the systems of "Facebook Inc") process data that "Facebook Inc" controls as a processor in the same facilities within the EEA, not the United States.

This is not to say that there may not be *individual* processing operation where personal data has to be transferred to the United States, but this complaint is dealing with the complete outsourcing of all processing operations by "Facebook Ireland Ltd" to "Facebook Inc".

Finally, it is obvious that the derogation in Article 26(1)(f) of Directive 95/46/EC does not apply.

## 6. Compliance with other Provisions of the DPA and Directive 95/46/EC

In addition to the issue of a third country transfer (under Art 25 and 26 of the Directive), "Facebook Ireland Ltd" has to comply with all other provisions of Directive 95/46/EC and the Irish Data Protection Act when transferring data to a processor and/or other controller.

This is also evident from the relevant Commission Decisions, that all clarify that these Decisions only apply "*without prejudice to* [the DPAs] *powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC*".

Despite the fact that "Facebook Ireland Ltd" and your office have so far only focused on the legality of the transfer under Articles 25 and 26 of Directive 95/46/EC and Section 11 of the DPA, your office will have to examine compliance with all other requirements of the law - just like any controller/processor transfer within the EEA has to comply with all legal requirements.

A transfer of personal data, where form of mass surveillance is, for example, a clear violation of Articles 6 and 7 of Directive 95/46/EC, as the Article 29 Working Party has already held in the equivalent SWIFT case (see Article 29 Working Party's Working Paper 128 from 22nd November 2013).

Most notably such a transfer violates (among other provisions) Section 2(1)(a) and 2D(2) "*fairly*" (2)(1)(c)(i) and (ii) "*purpose limitation*" (2)(1)(a)(iii) "*excessive*" and 2(1)(d) and 2C "*appropriate security measures ... against unlawful forms of processing*" of the Irish DPA and equivalent sections in Article 6 of Directive 95/46/EC. "Facebook Ireland Ltd" does also not fulfill any of the requirements in Section 2A DPA and/or Article 7 of Directive 95/46/EC and violates Section 2C(3) and 21 DPA and Article 17(2) and (3) of Directive 95/46/EC. To the extent that these provisions leave any room for interpretation, these provisions have to be interpreted in the light of Articles 7, 8 and 47 CFR, the Irish constitution and the clear judgements of the CJEU in C-362/14 and the High Court in *Schrems -v- the Data Protection Commissioner*.

# C. REQUESTS

## 1. Suspension of all data transfers

Based on the facts and legal arguments above – and any other legal or factual basis – I therefore request that the DPC issues a **prohibition notice** under Section 11(7) to (15) DPA, an **enforcement notice** under Section 10(2) to (9) DPA and/or any other appropriate step to suspend all data flows from "Facebook Ireland Ltd" to "Facebook Inc".

As I am clearly aware of the major consequences of such a decision, I would suggest issuing a decision with a reasonable implementation period in line with Section 10(5) and 11(10)(b) DPA that allows "Facebook Ireland Ltd" to take all necessary technical and organizational steps.

These steps may include processing all personal data within the EEA or any other third country (other than the United States of America) that provides "adequate protection" or e.g. rearrange its corporate structure (aimed at tax avoidance) to avoid the application of EU law.

The duration of such an implementation period will have to balance the practical possibilities with the fact that the "essence" of the fundamental rights of about a billion data subjects under Art 7, 8 and 47 CFR are continuously breached, as the CJEU has held in C-362/14 and the fact that "Facebook Ireland Ltd" had more than two years since the initial compliant to take the appropriate steps. It may be practical to use different periods for different processing operations that "Facebook Ireland Ltd" has outsourced to "Facebook Inc".

## 2. Copy of Agreements between "Facebook Ireland Ltd" and "Facebook Inc"

In addition, I hereby request that the DPC uses its powers under the DPA and Clause 8 of the Agreement of 20th November 2015 and any previous agreement to request a copy of all relevant agreements between "Facebook Ireland Ltd" and "Facebook Inc" and either forward these documents directly or order "Facebook Ireland Ltd" to forward these documents to me in accordance with Clause 4(h), or any other relevant clause, of the Agreements or the DPA.

## 3. Optional Audit of "Facebook Inc" and all Sub-Processors

Clause 8(2) of the Agreement of 10th November 2015 clarifies, that "Facebook Inc" and all "sub-processors" have submitted themselves to a right of your office to conduct an audit. This allows your office to audit all worldwide offices, data centres and documents of "Facebook Inc" and all "sub-processors".

I therefore request that you conduct an audit of the "data importer" ("Facebook Inc") and any sub-processor, if there is any doubt about the factual processing operations by "Facebook Inc" within the United States (or anywhere else in the world) and provide all parties to this procedure an option to engage in such an "audit" accordingly (which would clearly constitute an element of this complaints procedure).

### 4. Information about the Authorization of the Agreement

"Facebook Ireland Ltd" could have theoretically requested an authorization by the DPC under Section 11(4)(a)(ix) DPA of the altered agreement it presented to me. While I doubt that the DPC would and could have authorized this agreement under Section 11(4)(a)(ix) DPA and consequently informed the European Commission and all other European DPAs according to Section 11(4)(b) DPA, I hereby request a confirmation that the agreement presented was not authorized by the DPC.

## D. PROCEDURAL MATTERS

### 1. Access to Documents

I hereby refer to the exchange of letters between your office and my solicitor in relation to the access to all relevant documents, which you have chosen not to answer in any material way.

I assume that "Facebook Ireland Ltd" demands from your office that documents and evidence in this procedure kept secret. However your office is clearly not bound by Facebook's demands, but by Irish and EU law ensuring a fair procedure.

I await your directed response to my solicitor in this respect.

### 2. Proper Documentation

For the avoidance of doubt (and given previous experience with the DPC) I also kindly ask you to follow appropriate procedures that allow a fair and legally challengeable procedure.

I would therefore kindly ask you to e.g. refrain from "informal calls" or other non-traceable methods of conveying this complaint to "Facebook Ireland Ltd" or finding informal resolutions.

As previous court cases have shown that the DPC was in these cases unable to demonstrate it's (in)actions, which leads to massive legal uncertainty for all parties involved as well as the DPC.

### 3. Further Submissions Reserved

In the interest of a concise submission I have focused on the facts and issues that felt the most relevant and disputed. It should go without saying that an "update" to my original complaint is naturally only a first step in a procedure. A complainant cannot foresee your and Facebook Ireland's (often unorthodox) thoughts and arguments and must be able to address them in a "fair procedure".

Given the previous arguments by your office in *Schrems v. DPC*, in which you have repeatedly argued that I have not made certain factual submissions that only became relevant after your investigation and review of the complaint, I unfortunately feel that I also have to ask you to

follow appropriate procedures and revert back to me with counterarguments, factual matters not addressed and other such situations that may be a result of your investigation.

## 4. Judicial Review / Appeal

In relation to the procedural issues above (and indeed any other violation of a "fair procedure" and the law) I would like to highlight my determination, in the light of previous experiences with your office, to use all necessary and appropriate legal remedies to ensure that your office will undertake a proper investigation into this updated complaint and decide according to the law.

## 5. Misconduct in a public office

Finally, I unfortunately feel that it is appropriate to also highlight the personal criminal consequences for any officeholder that "*willfully fails to perform a duty that he is under*".

I understand very well, that your office is under massive political and economic pressure in this case. Given the very clear guidance by the High Court and the Court of Justice in C-362/14, and given my previous experiences, combined with very recent information I received about your offices' thoughts on this issue, it seems to be appropriate as a matter of fairness to inform you at the earliest possible stage of the possibility that your actions (or inactions) in this procedure may also have *personal* consequences for the relevant officeholder that go far beyond a mere appeal or judicial review against the decision of the office.

I hope I have assisted you with this "update" to my complaint to swiftly and comprehensively process my complaint that is pending since June 2013 and concerns one of the most massive violations of our fundamental right to privacy in human history.

In the course of this procedure may see a new "Safe Harbor" system to be established between the United States and the European Union which may be very helpful for many companies that relied on Decision 2000/520. Given the clear and binding decision by the CJEU on the basis of Articles 7, 8 and 47 of the Charter of Fundamental Rights in the case of "mass surveillance", as well as a number or other reasons, any such development must be clearly irrelevant for this procedure, which is why I rest assured that your office will deliver a decision in the near future.

Mag. Maximilian Schrems