Commission Nationale de
l'Informatique et des Libertés
8, rue Vivienne
75083 Paris
FRANCE

Maximilian Schrems
Schadekgasse 2/13
1060 Vienna
AUSTRIA

Brussels, Jan 28th 2016

To the Members of the Article-29-WP,

In advance of your meeting on February 2nd 2016 on the "Safe Harbor" situation, I would like to share with you the considerations below, which I hope will be of use for your further work.

A. Current Debate

1. Intensive Lobbying

I understand that the Article 29 WP is under severe and intensive lobbying from the business sector in the EU and the US. As there is no "Safe Harbor 2.0" at this stage, the industry is putting substantial pressure on all EU entities.

I very much encourage you to resist special interest and continue your work in protecting the fundamental rights of all data subjects under the European Union's jurisdiction.

The average data subject does not have the resources to bombard you with their views, paid "research" (that reaches from a mere repetition of the client's views to a full reinterpretation of the CJEU's judgment) or strategic PR (that goes so far as to claim that US privacy protections for non-US persons are more stringent than the EU's fundamental rights). I hope all members of the Article 29 WP will resist this pressure and will remain focused on the law and the facts.

2. Attempts to "reinterpret" the CJEU's ruling

A number of, mainly US-based and industry focused, lawyers have recently tried to intensively "reinterpret" the CJEU's ruling. In this respect, the following misinterpretations are repeated in a large number of their opinions:

Claim 1: "US must only be equivalent to the worst EU member state(s)"

Many commentators focus heavily on the CJEU's definition of "adequate" as being "essentially equivalent" and go on to argue, that any third country only needs to provide the minimal level of protection in any EU member state.

This view however disregards, that the CJEU has found, not only that Decision 520/2000 was invalid because it did not provide "essentially equivalent" protection, but also (and more importantly) because US law violated the "essence" of the Charter of Fundamental Rights.

The transfer of data has to pass two test: **1)** under Article 25 of Directive 95/46/EC the protection has to be "adequate" (meaning "essentially equivalent") and **2)** the protection has to fulfill the requirements of the Charter (most notably Art 7, 8 and 47).

As Article 25 of Directive 95/46/EC has to be interpreted in the light of the Charter, a lower level of protection by some EU member states is consequently absolutely irrelevant under a EU law. The recent "research" by paid "experts" is therefore flawed on the most fundamental level: All papers I am aware of compare US law against the "worst" member states – not against Article 7, 8 and 47 of the Charta of Fundamental Rights, which is the relevant benchmark within EU jurisdiction.

It may very well be that some EU member states violate the CJEU's interpretation of Articles 7, 8 and 47 of the Charter, but this does not mean that third countries are free to do the same or that the Charter of Fundamental Rights would be "undermined" by questionable surveillance practices of some member states. Even if some member states violate EU law, this does not give a third country the right to engage in similar violations of Fundamental Rights.

This situation may seem paradoxical for some, but it is based on the fact that the EU has no jurisdiction over "national security" of member states. It does, however, have jurisdiction over third country data transfers by private data controllers such as the companies involved in "PRISM".

The ECtHR in Strasbourg does have jurisdiction in these cases and will be addressed with the question of national surveillance programs in the near future, as well as courts and tribunals in the member states that are currently dealing with the fallout from the Snowden disclosures.

Claim 2: "US provide equivalent protection" / "New US laws in place"

The US representatives and lobby groups have produced extensive lists and summaries about so-called "changes" in US law. However, none of the elements and changes address the core concerns of the CJEU. Many "changes" are merely aspirational or obvious whitewashing. Changes like the "Freedom Act" do not address the relevant global US surveillance programs. Unfortunately, the United States has so far been unwilling and/or unable to pass any substantial change in its national surveillance laws, especially for non-US citizens, as most independent US scholars agree.

Without going into the details of all argument in this context, I would like to highlight that the US has not changed the relevant law and that the existing laws neither satisfy the CJEU's test employed in "Digital Rights Ireland" or "Safe Harbor" nor the ECtHR's test developed in settled case law and recently repeated in *Szabo and Vissy -v- Hungary* and *Zakharov -v- Russia*. I am not aware of any document or credible legal analysis that would show that US law (like e.g. 50 USC § 1881a, executive order 12333) would pass the clear case law developed by the CJEU or the ECtHR.

The numerous attempts of paid lawyer to argue that the US is in fact providing "essentially equivalent" protection are not supported by any factual evidence in US law.

Claim 3: "Factual Assessment by the CJEU was wrong"

Another argument used to call into question the decision of Europe's highest court, is that the CJEU and the Irish High Court have misunderstood US law and practices.

These claims are often focused on the finding of *"mass surveillance*" in the US. There is no clear definition of "*mass surveillance*" and a debate has emerged as to whether the mere collection, storage or access to data constitutes "*mass surveillance*", or not.

However the relevant paragraph 94 of the CJEU judgement does not find that "mass surveillance" violates Art 7 of the Charta, but any "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications"* does*.* It is beyond reasonable doubt that e.g. 50 USC § 1881a does allow for such "*access*" to data.

The CJEU did not rely on the finding that the US conducts "*mass surveillance*" but defined a clear benchmark for any form of access to content data, which some US laws obviously do not fulfill.

This is also in line with the definition of "processing" in Article 2(b) of Directive 95/46/EC, which is clearly defining "making available". This definition is also applicable for Article 8 of the Charter. Under US law, data controllers or processors obviously have to make personal data "available" to US authorities. A violation of Article 8 of the Charter is clarly fulfilled by the mere fact that data is "made available". This is also in line with the CJEU judgement in "Digital Rights Ireland" where the mere storage of data (which constitutes the processing operation before data is "made available") was seen as a violation of the Charter.

In summary the different attempts by lobby groups and the US government to "reinterpret" or "overturn" the clear judgement of the Union's highest court are fundamentally flawed.

B. Possible Paths towards Solutions

While I am hopeful that the European Commission and the US counterparts will find a solution on a successor to "Safe Harbor", it seems unclear (1) if a final deal can be reached, (2) if this deal can cover all processing operations and (3) when such a deal will come into effect. Therefore I would like to address possible solutions or approaches under the current situation and a new legal mechanism.

1. National Security: Separating "*problematic*" from "*non-problematic*" data flows

In the recent weeks and months, the debate centered on a potential "Safe Harbor 2.0" for all data transfers to the United States of America. However, little debate has focused on the core rational behind the ruling C-362/14, which was basically that certain US laws conflict with European fundamental rights under the Charter as interpreted by the CJEU – and, indeed, very likely also the European Convention of Human Rights (see *Szabo and Vissy -v- Hungary* and *Zakharov -v- Russia*).

This means that US data controllers or processors who fall under certain US surveillance laws like 50 USC § 1881a (among other laws) cannot be found to provide "adequate" (95/46/EG) or "essentially equivalent" (CJEU) protection from a standpoint of primary EU law – no matter which secondary law element the European Commission may introduce in the future and no matter what other "alternative" transfer method are used under Art 26(2) of Directive 95/46/EC.

However, laws like 50 USC § 1881a only apply to certain controllers (in the case of § 1881a only to "*electronic communications providers*"), but not all data controllers or processors in the US. The CJEU has not found that US law always conflicts with contractual or self-regulatory systems that aim at providing "adequate protection".

I would, therefore, like to encourage the Article 29 WP, to focus on solutions for data transfers to US data controllers that do not fall under any of these conflicting US surveillance laws, which would of course require a review of all relevant laws and their application. EO 12.333 does for example apply to all US entities, which is why the benefit of this approach may be limited.

2. Guidance on "Alternatives" (Standard Contractual Clauses / BCRs)

In the immediate response to the ruling C-362/14, many privacy and data protection experts and lawyers have encouraged data controllers to simply shift to SCCs or BCRs. Google and other providers have even sent mass-emails to all commercial customers claiming that the CJEU judgement in C-362/14 is irrelevant, because they also use SCCs.

In my view, even experts in the field have not properly examined the structure of the relevant decisions by the European Commission. The relevant Decisions 2001/497/EC, 2004/915/EC and 2010/87/EU all have an "exit door" that caters for exactly this situation, and allow DPAs to suspend data flows if

> "*it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the relevant data protection rules 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 standard contractual clauses*".

This section is taken from Art 4(1)(a) of Decision 2001/497/EC, the other decisions have similar exceptions. These exceptions refer to Article 13 of Directive 95/46/EC, which has to be read in the light of Articles 7, 8 and 47 of the Charter, as interpreted by the CJEU in C-362/14. The result of this legal

structure is clearly, that a European controller cannot rely on SCCs in the case of US mass surveillance laws that conflict with European fundamental rights.

In other words: A US law that led the CJEU to invalidate the "Safe Harbor" decision must also trigger the "exit doors" of the Commission Decisions 2001/497/EC, 2004/915/EC and 2010/87/EU.

Of course this matter is again only relevant if a US controller or processor falls under any of these US surveillance laws. Unfortunately, some of the largest IT providers (e.g. Apple, Microsoft, Google, Apple) fall under these laws and actively participate in these surveillance systems, as we know from the Snowden files. These laws equally apply to other IT companies, not named in the Snowden files.

I urge you to address the matter of SCCs and BCRs as "alternatives" with utmost clarity, as many data controllers are devoting large resources and time into this "quick fix" that does not provide the legal certainty many of them expect.

After the invalidation of "Safe Harbor" without any implementation period, it would be a second disaster for the trust of data controllers in EU institutions, DPAs and the rule of law, if they are led to believe that SCCs are a reliable fix in all cases, when in fact SCCs are subject to the limitations in the relevant Commission decisions given the exact same fundamental rights violation as in C-362/14.

3. Possible New Transfer Mechanism

If the European Commission and the US government are able to agree on a new mechanism to transfer data to the United States, this deal will have to stand the test by the CJEU. In this respect I would like to highlight that a new system must comply with Article 25 of Directive 95/46/EC and the Charter in two respects: Proper protection against government surveillance and "essentially equivalent" protection against the commercial use of data by certified companies.

It is obvious that the current "Safe Harbor Principles" are by no means even close to the rules for commercial data processing in Directive 95/46/EC. US companies would have to substantially change their data handling practices to comply with any new "essentially equivalent" data protection principles in a new mechanism. This will require a rather lengthy implementation and re-certification period. So far US companies have only certified compliance with the old "Safe Harbor Principles".

In respect to the question of US surveillance I can so far not see any substantial change in US laws and practices. I understand that a new deal will only be possible if it leaves the option for DPAs to suspend data flows whenever a US controller or processor falls under any overreaching surveillance laws ("exit door") - unless the negotiating partners are engaging in total denial of US laws.

Finally a new system will have to allow robust remedies in the private and public sector and proper overview by DPAs in order to comply with Article 8(3) and 47 of the Charter.

I would encourage the Article 29 WP to closely examine a possible new transfer mechanism in this respect to that any new system is not again unstable and likely subject to legal challenges.

C. Further Actions

Complaints

As some members of the Article 29 WP are well aware, there are a number of players (including myself) that will very likely continue to address these matters before DPAs or direct legal action where the situation remains to be unsatisfactory. This is why I would like to urge the Article 29 WP, in the interest of legal certainty and in order to settle the matter as far as possible, to focus on stable solutions that will withstand judicial scrutiny.

Clear Guidance

I would very much encourage the Article 29 WP to give clear and straightforward guidance to the vast majority of data controllers that are willing to comply with the law. Previous comments by various actors have often led to speculation, wishful thinking or even confusion. Being well aware of the rather diplomatic process within the Article 29 WP, I would also like to recall the crucial function of the Article 29 WP to provide for clear guidance.

While this may not be an option to the Article 29 WP, it seems that different views among the DPAs may be included in documents. It appears that it may be preferable to data controllers and data subjects in practice to deal with two or more straightforward views, than with a vague and unclear single text.

"Too big to shut down" Situation

Finally, I would like to address what I perceive to be the core problem of the judgement in C-362/14: The enormous factual consequences of enforcement actions. In simple terms: Some of these data controllers and processors seem "*too big to shut down*" (as banks were "*too big to fail*").

The US government uses international companies that have become worldwide utilities for mass surveillance. This leaves Europe in a deadlock: A prohibition of data transfers has enormous consequences for our daily life, but a continuous violation of our fundamental rights would however undermine our core values and the credibility of DPAs.

I would, therefore, encourage DPAs to find a balanced approach, which enforces our fundamental rights on controllers that knowingly violate them, but also allows "fade in" periods for data controllers to adapt to the CJEU ruling (e.g. by using reasonable implementation periods in orders). It would be a matter for each data controller to find the appropriate technical, organizational or legal solution in each situation and explain the necessary implementation periods to the satisfaction of the data protection authority concerned.

I hope this letter provided helpful input for the debate within the Article 29 WP and that it will help you to fulfill your core task of protecting our fundamental rights.

Maximilian Schrems