LIBE Committee Inquiry

on electronic mass surveillance of EU citizens

Public Hearing, Strasbourg, 7 October 2013

Contribution of Peter Hustinx (EDPS)

- Thank you for the invitation. The focus of your programme today is on the US Safe Harbour and other instruments for international data transfers, but I would like to use this opportunity to also make some general remarks on what is at stake, and what should be done in view of the various disclosures on electronic mass surveillance of EU citizens.

- When the first instalment of the NSA story had just been published in June, we immediately expressed our concerns about the possible serious implications for the privacy and other fundamental rights of EU citizens. We have asked for a profound explanation and clarification of the facts, we have insisted on immediate and adequate action, and we have been following the ongoing story ever since.

- Let me say that I am grateful for the steps taken by Vice-President Reding on behalf of the European Commission, and I very much appreciate the strong language used by Mrs Merkel and other European leaders.

- As you know, the Article 29 Working Party is currently involved in an assessment of the various surveillance programs, the consequences they

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

may have for the data protection of EU citizens and the implications this may have for international transfers. Our staff are actively contributing to this analysis, for instance on the applicability of EU law and the different issues arising in that context.

- At its last plenary meeting, only a few days ago, the WP29 gave a mandate to its relevant subgroups to continue their analysis of the various programs and report back to the plenary in December. The WP29 will then very likely be able to adopt a position on all relevant aspects of the matter.

- Although some of the facts are still not - and may in the end never be - sufficiently clear, this will not prevent us from investigating all relevant scenarios and analysing their consequences. Moreover, we also hope to benefit at some point from the findings and conclusions of other ongoing work.

- At the EDPS we are particularly concerned how EU institutions and bodies may have been affected, and we will be examining the possible need to increase current levels of information security, certainly also in view of the recent Belgacom story. In this context, we are intensifying our contacts with all relevant services.

- The three most striking points that we know at this stage are (i) the scale of the monitoring that has been going on, (ii) the number of private actors, including well known internet giants, that have apparently been involved, either actively or passively, and (iii) the development of weaknesses and backdoors in encryption, with far reaching perverse effects and very great damage to the public trust.

- At this stage, there seems to be little doubt that we are facing an existential challenge to our fundamental rights and liberties. We must therefore be prepared to *"draw a line in the sand"*.

- Strong safeguards for our privacy will need to be negotiated and adopted. If not, we will need to consider suspending data flows, and suspending or terminating existing agreements for data exchange.

- At the same time, it may be possible to develop more intelligent answers, turning a crisis into opportunities and using it positively, to our advantage.

- It seems to me that a first conclusion should be that there is now even more reason to decide on a swift adoption of the General Data Protection Regulation that will allow us to address the private actors much more effectively than under current legal frameworks.

- This means stronger arrangements for responsibility and accountability and for stronger and more consistent supervision and enforcement across the EU. It will thus also be essential to extend the scope of EU law to ensure a level playing field for all those active on the European market.

- The Regulation should also provide for a mechanism such as the famous Article 42 of a previous version, so as to address the real possibility of a conflict of international law, where jurisdictions have conflicting views of their public interests. The basic principle should be that all data flows must be in line with EU law, unless a binding international agreement has provided otherwise, or a judicial or supervisory authority has granted an exemption.

- Another point of attention is that an additional protocol to the Cybercrime Convention - as currently under discussion in the context of the Council of Europe - may well create space for unwarranted access by intelligence services to data stored in other jurisdictions. This issue has also been raised in the Opinion of the LIBE Committee for ITRE on the strategy for cloud computing. We should do our utmost to ensure that this additional protocol will not be adopted.

- The NSA story has also other implications which I can now only mention very briefly. If we are to *"draw a line in the sand"*, it should be to assert our European data protection culture, which does not discriminate on grounds of nationality. We can therefore not accept a distinction between US-persons and non-US-persons, which leaves all EU citizens without any proper legal protection.

- Another problem is the apparent large scale *collection* of data, subject only to restrictions on their *use*. This is totally incompatible with our emphasis on principles of necessity and proportionality when restrictions are imposed on fundamental rights.

- Let me therefore be very clear, we must now make a stand, it is really *"now or never"*.

- In this respect, it would not be so difficult to build a solid agenda for transatlantic discussion - and where necessary negotiation - on the way ahead. I would like to come back to this point at the end of my remarks.

- Let me now turn to the US Safe Harbour as one of the specific subjects for this hearing. Here, I would like to make my remarks in three steps:

first, the concept of "adequacy"; second, the "regular" US Safe Harbour; and finally, the exception for "national security" and similar interests.

- The notion of an "adequate" level of protection was included in Article 25 of the Directive in order to ensure data flows with third countries to be subject to sufficient protection, depending on the circumstances of the case, but not necessarily equivalent to the level of protection within the EU. That is a pragmatic approach reflecting the diversity of legal cultures in the world.

- The notion of "adequacy" has been further developed in an opinion of the Article 29 Working Party (WP 12) adopted in 1998, which has been the basis for all Commission decisions on adequacy, including the one on the US Safe Harbour. Adequate protection as referred to requires conformity with a core of "content" principles, and some "procedural / enforcement" requirements in order to ensure effective compliance, support and help to data subjects, and appropriate redress. In other words, an "objective" or "functional" approach.

- Among the content principles mentioned in the opinion are purpose limitation, data quality and proportionality, transparency, data security, rights of access and correction, and restrictions on onward transfers. However, the opinion also mentioned that exceptions could apply which *"should be in line with Article 13 of the Directive"* (see page 6). This Article 13 allows exemptions to protection for national and public security, to the extent necessary. Although this provision does not apply in a third country, it is relied on by analogy.

- In the context of contractual provisions to provide adequacy, the opinion also discusses the problem of "overriding law" (see page 21-22). One of

the conclusions is that *"countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers based on contractual clauses"* (see page 23). However, the same would of course apply to adequacy findings.

- The US Safe Harbour has been controversial from the very beginning. The WP29 has adopted a series of very critical opinions in the course of the negotiations between the Commission and the US Department of Commerce. However, once the negotiations were concluded and the Commission decision on the Safe Harbour was adopted, the WP29 has invested in bringing it to life and making it work better.

- Let me clearly say that the emphasis of Safe Harbour work for EU data protection authorities is at the national level. EU institutions and bodies sometimes transfer personal data to third countries, but this usually does not involve the Safe Harbour. However, from a strategic perspective, the evaluation is quite different. We have therefore been closely involved at different stages of the process.

- It is fair to say that the Safe Harbour made a slow start, but has gradually picked up momentum. We believe that substantial improvements have been made and most issues have now been settled. This is particularly true for the more active role of the US Department of Commerce in the self-certification process and for the role of the Federal Trade Commission in enforcement. So Safe Harbour therefore does have certain merits.

- What remains problematic is the lack of a comprehensive overview of SH practice and experience, together with sufficiently reliable statistics. For this reason, a Privacy Contact Group was established with representatives

from both sides, which has been active for a number of years. At this stage, the WP29 is looking forward to the assessment report which has been announced by European Commission.

.

- According to the introductory part of the Safe Harbour Principles (see annex I to the Commission Decision of 26 July 2000), adherence to these principles may be limited: *"to the extent necessary to meet national security, public interest, or law enforcement requirements ..."*. There is also a similar provision that deals with overriding law. However, it is good to keep in mind that we are dealing in this context with exceptions to fundamental rights, which the Court of Justice and the European Court of Human Rights always interpret restrictively.

- Moreover, the text referred to is carefully crafted language - with the words *"to the extent necessary"* - whereas in the current situation we seem to be confronted with systematic non-compliance with SH principles in all cases where companies may have been approached under any of the mass surveillance programs.

- Both sides may well disagree on whether this exception in fact applied. In any case, this question should be answered in the negative, if we assume that the relevant surveillance programs were indeed excessive. Again, it is likely that both sides will disagree about that conclusion.

- This could be a reason to invoke Article 4 of the Commission Decision, according to which that decision *"may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles (...) is overtaken by the requirements of US legislation."* Any relevant evidence could for instance be provided by a

Commission evaluation report such as the one expected by the end of the year.

- Any further steps should then be taken by the Commission together with the Article 31 Committee of Member States' representatives. In that case, the focus will be more on *"how to deal with excessive surveillance"* or *"disagreement on that subject"* than on the effectiveness of the SH as an instrument for adequate protection. However, the Commission report could address both and thus provide substantial input for discussion and negotiation with the US side. In that context, let me say that we should not throw away Safe Harbour as such without investigating the scope for improvements.

- An agenda for improvements of the SH *"in the light of experience"* could be combined with other issues and concerns, either in the context of law enforcement cooperation or trade, or in the long term perspective of a new international agreement with principles for lawful surveillance,

- In this context, we should not fully exclude that a significant part of the solution may come from the US side. It may be recommendations from the US Privacy and Civil Liberties Oversight Board or from the internal expert group established by the US Administration on more transparency or other meaningful safeguards.

- In any case, it would be wise to keep all options open, and at the same time also explore all relevant possibilities for a constructive engagement.

* * * * *