EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

12.12.2013

WORKING DOCUMENT 4

on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Axel Voss (Co-author)

Impact of US Surveillance programmes on transatlantic agreements

Given the scale of the revelations on US surveillance activities, EU citizens expect the European Parliament, as the only directly elected institution in the European Union, to act. Parliament should not just react to these revelations but should instead engage in a mature investigation based on sound legal principles and fact finding to thoroughly analyse the legal framework for data transfer with the US. Transatlantic data transfer does not take place in a grey zone outside a legal framework; instead several existing transatlantic agreements apply.

As a consequence of the US surveillance activities several political actors called for the suspension of some existing transatlantic agreements. Drawing conclusions from the LIBE Inquiry Committee on Electronic Mass Surveillance of EU Citizens and the LIBE delegation to Washington D.C. in October 2013 it is clear that in order to restore trust in the transatlantic relationship we have to strengthen the economic transatlantic cooperation and to ensure an adequate balance between the fundamental right of EU citizens to data protection and the lawful pursuits of law enforcement.

As the LIBE Inquiry Committee on Electronic Mass Surveillance of EU Citizens is ongoing and will present the final document early 2014, the focus of this working document will be on existing transatlantic agreements that differ in terms of their scope, content and legal application. The TFTP Agreement, the EU-US PNR Agreement and Safe Harbour are three completely different agreements regulating data flows with the US. On one hand, the TFTP and the EU-US PNR are agreements in the field of justice and home affairs and tools in the fight against globalised terrorism and serious crime. On the other hand, Safe Harbour is a mechanism for data transfers in the business sphere.

Safe Harbour

The Safe Harbour is a mechanism put in place by the US authorities (Department of Commerce, Federal Trade Commission and Department of Transportation) and the European Commission in order to provide U.S. companies processing personal data of European citizens' with a tool enabling them to transfer data to the US while providing an adequate level of protection. The US Safe Harbour was established to address the problem raised by the lack of adequacy of the US privacy legal framework.

Safe Harbour allows an EU controller to transfer personal data to a US organisation that has self-certified adherence to the Safe Harbour and commits to ensure compliance with the Safe Harbour Principles. Safe Harbour has been a matter of political controversy from the very beginning. The European Parliament emphasised several concerns based on the absence of an individual right of judicial appeal, the lack of obligation on companies to pay compensation for unlawfully processed data and the different protection systems that existed in the US which depend on whether or not the owners of the data are European.

In case of a breach of the Decision 2000/520/EC it implies a twofold system for suspension or termination of the mechanism. According to Article 3 the data protection authorities of the Member States may exercise their existing powers to suspend data flows to an organisation in cases where there is a substantial likelihood that principles are being violated and processing of personal data or the continuing transfer would create an imminent risk of grave harm to data subjects. The Member States must inform the European Commission in such cases. The

European Commission is required to evaluate the implementation of the decision on the basis of available information and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC. Consequently the Commission may state that the implementation or the functioning of Safe Harbour does not work and it may propose measures for instance to suspend or to revoke the decision.

Safe Harbour is today considered as a possible obstacle for the enforcement of EU data protection rules. In addition, it is suspected to serve as one element in the chain of legal justifications for the US mass surveillance program PRISM. It was only after the media disclosed the NSA mass surveillance activities and the fact that it emerged that major US electronic communication companies, all of them self-certified under Safe Harbour, were involved in these activities, that the European Commission publicly announced an evaluation of the US Safe Harbour. This subsequent evaluation[1] importantly recognises the need to review Safe Harbour taking into account the new context of technologies with the exponential increase in data flows, the increased importance of data flows notably for the transatlantic economy, the rapid growth of the number of companies in the US adhering to Safe Harbour and the information recently released on US surveillance programmes. The communication outlines 13 key recommendations to be implemented by the US to address the fundamental shortcomings identified which will provide the basis for a full review into the functioning of the Safe Harbour principles.

However, despite this reaction by the Commission, concerns have been raised as to the adequacy of the Safe Harbour given the extent of mass surveillance on private behaviour. In terms of electronic mass surveillance of EU citizens by the NSA, there is widespread political agreement that the European Union should aim at ending the adequacy determination of the Safe Harbour and finding new legal solutions. The Report of the ad hoc EU-US Working Group on data protection of 27 November 2013 confirms[2], states that US law does not confer on non US persons any judicial or administrative avenue as regards access, redress and information on their personal data being processed for law enforcement or national security purposes. The Safe Harbour is no longer "safe".

The suspension or termination of the Safe Harbour Agreement is also a political debate, but would possibly lead to economic consequences. The US and the EU are important economic partners. Thus, it is more than important to rebuild the mutual trust between the transatlantic partners, to strengthen the trust in the economy and more specifically to adopt common or adequate data protection standards on both sides of the Atlantic. In the long term it could also contribute to restoring the transatlantic relationship to a more solid basis. However, the effect of possible economic consequences remains to be seen. All the major US internet companies could be seriously affected should the EU decide to repeal the Safe Harbour decision of 26 July 2000. They would be required to use other instruments laid down by Directive 95/46/EC, e.g. contractual or binding corporate rules. However, national data protection authorities should consider whether these instruments provide adequate protections, taking account of US law on intelligence and national security and the involvement of these companies on mass surveillance activities of US intelligence agencies.

[1] Communication from the Commission to the European Parliament and Council on the Functioning of Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013)847, 27.11.2013.

[2] Council document 16987/13, 27 November 2013."... There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress"

TFTP Agreement

The TFTP Agreement between the European Union and the US on the processing and transfer of financial messaging data from the EU to the US for the purpose of the Terrorist Finance Tracking Program (hereinafter 'the TFTP Agreement') was concluded on 13th July 2010 and entered into force on 1st August 2010.

Terrorist finance tracking is an essential tool in the fight against terrorism financing and serious crime, allowing counter terrorism investigators to discover links between targets of investigation and other potential suspects connected with wider terrorist networks suspected of financing terrorism. Following a long negotiation process, the European Parliament agreed to the TFTP agreement on the basis that that the agreement provided a balanced approach to fighting terrorism and, at the same time, guaranteed the protection of civil liberties and fundamental rights and ensuring the privacy and data protection.

The allegations of NSA tapping into the SWIFT database have raised serious concerns as to whether the agreement offered real legal guarantees and safeguards for EU citizens' personal data. There were calls across the political spectrum for the European Commission to investigate fully the allegations of serious breaches of the EU-US TFTP agreement in order to restore trust and loyal cooperation in the transatlantic relationship with the US. In a Joint Resolution on the SWIFT agreement as a result of US National Security Agency surveillance[1], the majority of the European Parliament voted in favour of the European Commission suspending the current agreement.

According to Article 21 of the TFTP Agreement a suspension of the agreement is legally possible: "Either Party may suspend the application of the agreement with immediate effect, in the event of breach of the other Party's obligations under the TFTP Agreement, by notification through diplomatic channels. Termination shall take effect six months from the date of receipt of such notification. Besides the Parties shall consult prior to any possible suspension or termination in a manner which allows a sufficient time for reaching a mutually agreeable resolution. Notwithstanding any suspension or termination of the TFTP Agreement, all data obtained by the U.S. Treasury Department under the terms of this Agreement shall continue to be processed in accordance with the safeguards of the Agreement, including the provisions on deletion of data."[2]

The US Department of the Treasury, in reply to Commissioner Malmström and to the LIBE Delegation to Washington D.C.(28-30 October 2013), officially stated that the US government (the NSA is in that sense considered part of the government) has not been collecting and processing SWIFT data in any other way than as recognised in the agreement. The US Department of the Treasury also gave assurances in relation to access to SWIFT formatted messages in accordance with other legal tools in place.

[1] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0449&language=EN&ring=P7-RC-2013-0468

[2] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Official Journal of the European Communities L 215/7; 25.8.2000.

Commissioner Malmström reported to the members of LIBE Committee on the recent developments in TFTP and TFTS on 27th November 2013. In the framework of the consultation procedure within the TFTP agreement, Commissioner Malmström has had a number of contacts with the US and those consultations have not revealed any elements indicating a breach of the TFTP Agreement by the US.. Furthermore, they have led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the TFTP agreement. Europol and SWIFT officials reported to the LIBE Inquiry Committee that there were no indications for a breach of the TFTP Agreement by the NSA.

Despite these assurances from the US and the Commission, concerns have been raised by certain political groups as to the clarification provided, given the lack of any technical investigation and the reliance on statements issued by the US. Trust needs to be re-established to allow for future, successful cooperation between the US and the EU.

EU-US PNR Agreement

The EU-US Passenger Name Record Agreement (hereafter 'EU-US PNR') was concluded under Article 24 and Article 38 of the former Treaty of the European Union. The PNR are data-sets which are created for every flight passenger by airlines in a computer reservation system. The US-EU PNR is an agreement of the EU with a third country and thus subject to approval by the European Parliament. The new agreement was concluded in November 2011 and includes a clear scope, maximum time for the storage of data, the possibility for EU officials to inspect the implementation of the agreement in the US and a review clause

The EU-US PNR Agreement contains a suspension and a termination clause. On the one hand Article 24 allows the suspension of the agreement in cases of any dispute arising from the implementation of the agreement and many matters related thereto. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of the agreement by written notification through diplomatic channels, with any such suspension to take effect 90 days from the date of such notification, unless the Parties otherwise agree to a different effective date. Notwithstanding any suspension of the EU-US PNR Agreement, all PNR obtained by the United States Department of Homeland Security (DHS) pursuant to this Agreement prior to its suspension shall continue to be processed and used in accordance with the safeguards of this Agreement. However, it should be noted that a breach of an agreement may be considered a crucial factor and could lead to a suspension of the agreement. On the other hand Article 25 of the EU-US PNR Agreement is the termination clause of the legal agreement. Either Party may terminate the agreement at any time by written notification through diplomatic channels. Termination shall take effect 120 days from the date of such suspension.[1]
Given the serious concerns raised in the EU about US surveillance programmes, the European Commission issued the joint review of the implementation of the Agreement between the EU and US on the processing and transfer of PNR to the DHS to verify how these agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data

[1] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security; Official Journal of the European Union L 215/5; 11.8.2012.

protection experts from the EU and the US, looking at how the Agreement has been implemented.

According to this final report[1] "DHS has declared that it shares PNR with the U.S. Intelligence Community if there is a confirmed case with a clear nexus to terrorism and always under the terms of the Agreement. During the review period, DHS made 23 disclosures of PNR data to the US National Security Agency (NSA) on a case-by-case basis in support of counterterrorism cases, consistent with the specific terms of the Agreement". According to the review, sharing data with third countries is interpreted strictly, and also in line with the agreement. Consequently, according to the review, there are no elements indicating a breach of the EU-US PNR Agreement. However, the final report does not mention the fact that in the case of processing of personal data for intelligence purposes, under US law non-US citizens do not enjoy any judicial or administrative avenue to protect their rights. Constitutional protections are only granted to US persons.[2]

US Surveillance programmes and their impact on future transatlantic agreements

As a result of the revelations of US mass surveillance, there is a need for trust to be restored and reinforced in EU-US transatlantic relations. In terms of future transatlantic agreements, there must be a relationship of trust to allow for cooperation between both sides to find agreement on issues important to both EU and US citizens. It is imperative that the US recognises that respect of fundamental rights and data privacy is an essential element of EU and Member States legal framework and a major concern in the EU. The lack of satisfactory controls to guarantee data security for EU citizens and companies in Europe will negatively impact on future transatlantic agreements. The access to information processed and stored in the EU, either directly by US NSA or other intelligence agencies, or without using the mechanisms for mutual legal assistance, has seriously eroded the transatlantic trust and also impacted on trust of US organisations acting in the EU. This is all the more exacerbated by the lack of judicial and administrative remedies for redress of US law for EU citizens, particularly in cases of surveillance activities for intelligence purposes. When considering its importance in transatlantic agreements, the European Parliament should re-evaluate its role to ensure that the responsibility does not end after supporting an agreement. As a democratically elected institution, the European Parliament is obliged to ensure that the fundamental rights of EU citizens are respected and continue to be respected in any transatlantic agreement.

Recommendations;

The EU and the US approach to data protection and privacy fundamentally differ from each other. Whereas data protection is a fundamental right in the EU, it is perceived as an element of consumer protection and organised in a sectorial way in the US. Whilst within the EU there

[1] Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security Accompanying the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security SEC(2013)630final, Brussels 27.11.2013.

[2] Report of the EU-US Working Group on data protection. Council document 16987/13, 27 November 2013.

is a constant effort to balance data protection and privacy on the one hand and security and law enforcement on the other, the US seems to give only priority to security and law enforcement.

The surveillance activities by the NSA have primarily an impact on the EU citizens' privacy but also on the relations between the US and EU. US surveillance activities, with respect to EU data, might have legal implications on the existing transatlantic agreements and on future transatlantic cooperation. A lack of trust and tensions between the transatlantic partners are consequences resulting from the breach of legal agreements between the US and EU. (Temporary) suspension and renegotiations of existing economic transatlantic agreements might be a possible legal implication resulting from US surveillance activities. As mentioned already, this refers to the above proposal of ending Safe Harbour in order to balance the transatlantic relationship. In relation to this, the European Commission is strongly urged to conclude the on-going negotiations on a data protection agreement for law enforcement purposes (umbrella agreement). This agreement is of utmost importance as and it would act as the basis to facilitate data transfer in the context of police and judicial cooperation and in criminal matters; moreover it would give EU citizens the right to judicial redress in the US whenever their personal data are being processed in the US for law-enforcement or judicial cooperation purposes. This agreement should enforce data protection and privacy rights of EU citizens' whilst restoring trust in transatlantic cooperation in the field of justice and home affairs.