EUROPEAN PARLIAMENT 2009 - 2014

Committee on Foreign Affairs

4.11.2013

DRAFT WORKING DOCUMENT

on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens

Committee on Foreign Affairs

Rapporteurs: José Ignacio Salafranca Sánchez-Neyra, Ana Gomes, Annemie Neyts-Uyttebroeck

Preliminary findings:

1. Cooperation between the United States and the European Union and its Member States in counter-terrorism remains vital for the security and safety of both, the US and the EU. Also, given the state of modern technologies which can be misused for terrorist and criminal purposes, it is of crucial importance that intelligence services and law enforcement agencies on both sides of the Atlantic are able to use digital technologies to prevent disastrous criminal acts.

   However, with the revelations about massive electronic surveillance and systematic collection of communication data of EU citizens by the US National Security Agency going beyond any probable cause or reasonable suspicion of criminal activity, and about US spying on phones of political representation of allied NATO/EU countries, the trust of Europeans in the transatlantic partnership and in its shared basic values is seriously damaged.

   Moreover, in light of the technologies available and the revelations about activities of US and some European intelligence services, many citizens consider the open, democratic character of our societies to be in danger. It is the task of public authorities, both in the EU and the US, to re-establish the balance between security and privacy. There is a danger of the development of a surveillance state, given growing data processing capacities of computers and availability of any kind of information on social networks. The individual risks being completely known and his behaviour predictable by the state.

   Given that EU treaties allocate the responsibility to define the framework for the protection of personal data in the Union at the EU level, the EU must ensure that its citizens have information and judicial redress rights in case of data misuse - both within the EU, and also with regard to data collected and processed by and in the US.

   Cooperation among intelligence services remains a competence of EU Member States. However, the EU institutions need to strengthen their ability to defend themselves against spying activities.

2. The Snowden materials and related journalistic investigations published since June 2013 have disclosed massive electronic surveillance by US and some European intelligence services. Whereas there are legal limitations on the collection of data of US citizens by US intelligence services, laws enacted after 9/11 (mainly the US PATRIOT ACT and the Foreign Intelligence Surveillance Act - FISA) allow for principally limitless surveillance of non-US citizens. The purpose of surveillance of non-US persons is very broadly defined, far beyond counterterrorism purposes (“foreign intelligence information”, “necessary to the conduct of the foreign affairs of the United States”). The 4th Amendment to the US Constitution (which prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause) has been interpreted as applying to US citizens only. Non-US persons have no rights and no protections as their data are swept up and collected by the NSA.

   As top representatives of US Administration and Members of US Congress admitted, the scale and scope of NSA surveillance conducted violates the US Constitution and rights of American citizens, and goes far beyond measures required for counter-terrorism purposes.

US authorities also admitted that congressional and judicial oversight of these intelligence operations failed. President Obama instructed two bodies to review the ongoing surveillance programs so as to find a new balance between security and privacy, and strengthen transparency and protections against abuse. Also, a debate in Congress about the scale and scope of surveillance and about appropriate judicial and congressional oversight is ongoing.

3. However, the US debate is solely focussed on remedies needed to strengthen the rights of US citizens. Although US providers of web-based services and network equipment manufacturers receive significant shares of their revenues from overseas clients, the discrimination against non-US citizens has so far not been addressed in Congressional and public debate. The European legal framework (ECHR, EU Charter of Fundamental Rights) to the contrary does not discriminate, as far as privacy rights are concerned, on the basis of citizenship – privacy rights are given to "every person."

   International law, however, obliges the US to respect the universality of privacy rights and prohibits discrimination: the US is party to the International Covenant on Civil and Political Rights which, in its Article 17, provides for universal protection of the rights of privacy, and prohibits gathering and holding of personal information, except where authorised by law.

4. With the damage to trust in the transatlantic relationship caused by NSA massive surveillance and lack of data privacy remedies for Europeans, the transatlantic economic relationship is at risk.

   The EU and the US are pursuing negotiations for a Transatlantic Trade and Investment Partnership, which is of major strategic importance for creating further economic growth and for the ability of both, the EU and the US, to set future global regulatory standards. However, given the importance of digital economy in the relationship, it is crucial that agreement on strong data privacy protections is achieved separately from the TTIP.

   It was, interestingly, an appeal by US internet and digital technology companies and by US civil society to the US Administration and Congress, which put American citizens and international users of US-based service providers at the same level of legitimate need for greater transparency around national security-related requests by US government to service providers for information about their clients. Estimates elaborated by US researchers indicate that, as consequence of mistrust caused by NSA programmes, $180 billion or 25% of US overseas information technology services risk to be lost by 2016[1].

5. The crisis of trust risks spill over to other transatlantic instruments such as the EU/US Safe Harbour Decision of 2000. The Commission report assessing the Safe Harbour Agreement is expected to be published before the end of 2013. Other agreements concluded among the transatlantic partners remain important instruments in transatlantic cooperation (TFTP/SWIFT, PNR, etc.). However, should they be preserved, they have to be examined, weaknesses identified and data privacy protections strengthened.

[1] Results of research by Forrester Research Inc., Cambridge, Massachusetts, reported in http://www.bloomberg.com/news/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html

6. The Snowden materials also revealed information about US spying activities against EU institutions and EU Delegations on US soil. Such activities are inacceptable among allies. These revelations must however create an incentive for the EU institutions to strengthen their ability to defy spying activities directed against them.

7. The results of the dual track approach adopted by the Council are pending:

   - The EU-US ad hoc working group on data protection issues has held several rounds of meetings; the EP has however not received any results so far. Also, concrete answers to questions formulated by Commissioner Reding in her letter to Attorney General Holder are pending. It is important that the remedies needed for EU citizens with regard to electronic surveillance are addressed publicly, at the political level.

   - Also, bilateral communication between some EU Member States and the US authorities on spying allegations are pending.

   In addition, the EU Commission should clarify with the US authorities the allegations of spying against EU institutions and facilities.

8. Revelations on NSA activities allegedly conducted against top state representatives and important companies considerably strained US-Brazil and US-Mexico relations. The first state visit of the President of Brazil to the US for several decades has been cancelled. An investigation by the National Congress of Brazil is ongoing. These are likely not the last diplomatic incidents as more revelations are likely to come out, possibly causing more problems for the US and also possibly for EU Member States.

   The Snowden revelations have turned away the focus from cyber activities of state sponsors of cyber crime who do not share the same value base as the transatlantic partners do, and also from non-state criminal groups. The ongoing discussion should be an opportunity for the EU and the US to engage in joint efforts to upgrade the international legal framework on data privacy and on cyber security, and also to step up cooperation to be able to face these dangers.

Preliminary recommendations:

1. The ongoing debate is an opportunity to develop, in light of the technologies available, a new balance between security and privacy, both within the EU and also in the transatlantic partnership. The adoption of an improved EU data protection legislative package would be an important step in this regard; the Council is urged to speed up its work on this legislation.

2. It is vital that transatlantic cooperation in counter-terrorism continues; however, clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the transatlantic partnership. Therefore, an EU-US agreement protecting the privacy of citizens and allowing for equal rights in terms of information and judicial redress rights for European and American citizens is needed. The ongoing negotiations on an EU-US data privacy umbrella agreement are an important opportunity in this regard.

   The EU's task is to actively engage US counterparts so that in the ongoing American

political debate on reforming surveillance and reviewing intelligence oversight, the privacy rights of EU citizens are addressed, equal information rights and privacy protections in US courts are guaranteed and the current discrimination is not perpetuated.

Also, appropriate legislative changes should be undertaken and effective guarantees given to Europeans ensuring that the use of surveillance and data processing for foreign intelligence purposes is limited by clearly specified conditions, related to reasonable suspicion or probable cause of terrorist / criminal activity; this purpose has to be subject to transparent judicial oversight.

3. In parallel, the EU-US cooperation should facilitate development of international norms at the UN level to tackle the transnational character of data protection, including specific provisions defining limitations to privacy rights with regard to national security. The efforts by the German government to propose in this regard an additional protocol to the International Covenant on Civil and Political Rights should be actively supported by the EU, including by the EU Delegation at the UN.

4. The IT Security of EU institutions, including the EEAS and the network of EU Delegations needs to be strengthened, a system of secure communication built up. Assessments of related budgetary needs should be elaborated and first measures taken without delay. Appropriate funds need to be allocated in the 2015 Draft Budget.

5. The EU institutions should explore the possibilities for negotiating an EU-US anti-spying agreement.