EUROPEAN PARLIAMENT 2009 - 2014

*Plenary sitting*

1.7.2013 B7-0341/2013

# MOTION FOR A RESOLUTION

to wind up the debate on the statements by the Council and the Commission

pursuant to Rule 110(2) of the Rules of Procedure

on the US National Security Agency surveillance programme, surveillance bodies and programmes in various Member States and their impact on EU citizens' privacy
(2013/2682(RSP))

**Marie-Christine Vergiat, Cornelia Ernst, Kyriacos Triantaphyllides, Takis Hadjigeorgiou, Mikael Gustafsson, Willy Meyer, Nikolaos Chountis, Patrick Le Hyaric, Alda Sousa, Marisa Matias**
on behalf of the GUE/NGL Group

**B7-0341/2013**

**European Parliament resolution on the US National Security Agency surveillance programme, surveillance bodies and programmes in various Member States and their impact on EU citizens' privacy**
**(2013/2682(RSP))**

*The European Parliament*,

– having regard to the European Convention on Human Rights, especially its Articles 7 and 8, and to the EU Charter of Fundamental Rights, especially its Articles 48 and 52,

– having regard to the Agreement on Mutual Legal Assistance between the European Union and the United States of America[1],

– having regard to the Convention on Cybercrime (CETS No 185),

– having regard to the International Covenant on Civil and Political Rights, in particular Article 17 thereof on interference with any person's privacy, family, home or correspondence,

– having regard to the Vienna Convention on Diplomatic Relations, in particular Articles 24 and 27 thereof on the inviolability of diplomatic documents and communications,

– having regard to the EU-US Safe Harbour Agreement, in particular Article 3 thereof, and to the list of participants in the agreement,

– having regard to its resolution of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (Echelon interception system)[2] and the relevant report of its Temporary Committee on the Echelon Interception System (A5-0264/2001),

– having regard to the debate with Commissioner Reding on 15 February 2012 on third-country legislation and EU data protection laws (PV 15/02/2012 - 19),

– having regard to Directive 2002/58/EC on privacy and electronic communications,

– having regard to the data protection package consisting of proposals COM(2012)0011 and COM(2012)0010,

– having regard to the ongoing negotiations on the EU-US agreement for the protection of personal data exchanged for law enforcement purposes,

– having regard to the Commission communication on unleashing the potential of cloud computing in Europe (COM(2012)0529),

– having regard to the EU-US TFTP (Terrorist Finance Tracking Programme) Agreement

[1] OJ L 181, 19.7.2003, p. 34.
[2] OJ C 72 E, 21.3.2002, p. 221.

and the EU-US PNR (Passenger Name Records) Agreement,

– having regard to Rule 110(2) of its Rules of Procedure,

A. whereas newspapers across the world have revealed the existence of a US programme called PRISM, following information leaked by Edward Snowden, a former NSA intelligence officer who is now applying for political asylum , which allegedly entails the surveillance of communications of non-US citizens, hence including also European citizens, on a vast scale;

B. whereas Commissioner Reding has sent the US Attorney General, Eric Holder, a letter raising European concerns and asking for clarifications and explanations regarding the PRISM programme and other such programmes which involve data collection and search and the laws under which such programmes may be authorised;

C. whereas the abovementioned leaks reveal that EU Member States were allegedly cooperating in the US-led PRISM Programme or have developed similar intelligence-gathering programmes, such as the 'Tempora' Project led by the UK's Government Communications Headquarters (GCHQ); whereas press reports have revealed that GCHQ has tapped into undersea fibre-optic cables to obtain access to telephone conversations and internet traffic under a programme codenamed TEMPORA, basing itself on paragraph 4 of section 8 of the Regulation of Investigatory Powers Act (RIPA), which allows the UK Foreign Secretary to issue a certificate for broad interception of categories of material relating to terrorism or organised crime; whereas there is evidence which indicates that the US has been involved in spying on diplomatic personnel of the Permanent Representations of the Member States, as well as the offices of the EU institutions; recalls, in this regard, the bugging of an MEP's office by the British security services;

D. whereas the mass collection and retention of personal data is in itself contrary to the proportionality and necessity standards of the ECHR, according to which any restriction of fundamental rights needs to be proportional and necessary in a democratic society;

E. whereas Article 48 of the Charter underlines the presumption of innocence, and whereas in the absence of any formal accusation or charge, preventive policing or surveillance poses a great risk of violation of the presumption of innocence where it takes place on a vast scale without any prior existing evidence of criminal conduct;

F. whereas Article 52 of the Charter states: 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others';

G. whereas the European Court of Human Rights has rightly warned that a system of secret surveillance for the protection of national security 'may undermine or even destroy democracy under the cloak of defending it', and that 'the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied';

H. whereas, under the Safe Harbour Agreement, the Member States and the Commission are entrusted with the duty of guaranteeing the security and integrity of personal data; whereas, under Article 3, the Commission has a duty, should the provisions of the agreement not be respected, to reverse or suspend the agreement;

I. whereas the Data Protection package is currently being discussed by the two co-legislators;

J. whereas severe doubts exist about the willingness of some Member States, most notably the UK, to engage in a constructive manner with the Data Protection Directive in the law enforcement sector in order to improve the data protection standards in the field of police and judicial cooperation;

K. whereas the draft Data Protection Regulation, as sent in November 2011 by Justice Commissioner Viviane Reding to her colleagues, contained a provision that would make it a condition for the disclosure of user data to authorities in third countries to have a legal foundation such as a mutual legal assistance agreement and an authorisation from the competent data protection authority;

L. whereas strong lobbying by the US has taken place, which may have led to securing the removal of those provisions from the final Commission draft;

M. whereas EU Member States are bound to respect fundamental values as enshrined in Article 2 TEU, as well as the rights of privacy and data protection as stipulated in the Charter of Fundamental Rights;

N. whereas Parliament has rejected the Commission proposal for the setting-up of a European PNR scheme, given that serious concerns exist regarding the legality, necessity and proportionality of such a scheme;

O. whereas the Data Retention Directive has been challenged before constitutional courts and has now been referred for a preliminary ruling to the European Court of Justice, on grounds relating to proportionality and necessity;

P. whereas the European Parliament is currently debating the new Europol regulation;

1. Is profoundly shocked at the revelations concerning the existence of the PRISM programme, as it would, if the information available up to now is confirmed, entail a violation of the fundamental rights to privacy and data protection of EU citizens, and a violation of the core principles of necessity and proportionality;

2. Considers that there are reasonable grounds to believe that the communications of the European Parliament, its Members and staff have been intercepted by the TEMPORA Programme in a way that breaches the UK's human rights obligations; instructs its Legal Service, therefore, to explore the possibilities of legal action by the European Parliament against the UK Government, including through the European Court of Human Rights;

3. Calls for the immediate suspension of negotiations on the Transatlantic Trade and Investment Partnership (TTIP) agreement with the US; calls on the Commission to suspend any further negotiations on, or implementation of, the Free Trade Agreement

(FTA) with the USA until Parliament has been fully informed on this issue, the EU-US Data Protection Agreement has been satisfactorily concluded and effective guarantees are presented that the unlawful surveillance of EU companies, EU citizens and EU institutions and diplomatic representations have effectively stopped;

4. Recalls the principle of the presumption of innocence, which is an essential cornerstone of the rule of law in democratic societies; expresses its strong opposition to the increasing use of so-called 'preventive policing', which reverses the presumption of innocence and treats every individual as a potential criminal;

5. Is deeply concerned at the ever more security-led policies of the EU and the Member States which are drastically undermining the fundamental rights and freedoms of EU citizens and residents; is categorically opposed to the fear-led philosophy which seems to believe that more and more security will automatically result in an area of freedom and justice;

6. Calls on the US authorities to provide information to their EU partners, both at EU and Member State level, on the scope of the PRISM programme, the existence of similar programmes, and the level of involvement of EU Member States; also calls on the Member States to disclose the existence of any such programmes currently operating or under development;

7. Recalls the limits established by ECtHR case law in relation to state surveillance of individuals, namely that interference with the fundamental right to privacy of citizens must be of a nature that is proportionate and necessary in a democratic society, may only take place within the limits of the law, and must be embedded in appropriate democratic and judicial oversight;

8. Recalls the principle of proportionality as enshrined in the Cybercrime Convention, signed by the US, which stipulates in its Article 15 the obligation to respect the principle of proportionality when implementing measures aiming at achieving cyber-security;

9. Reaffirms the right of citizens to know of the existence of laws or policies which entail the risk of restrictions on their fundamental rights and freedoms, and to hold those who have implemented them to account;

10. Calls on the Council to accelerate its work on the Data Protection Directive, an instrument which is absolutely necessary to guarantee the rule of law and protect citizens' rights in the law enforcement field;

11. Calls on the EU's co-legislators to take a horizontal approach towards legislative proposals on law enforcement policies involving the collection and retention of personal data, especially the EU's PNR and Europol proposals, instead of adopting a piecemeal approach which risks creating a unworkable maze of incoherent standards and principles;

12. Calls for the formalisation of Parliament's stance against adopting further measures on law enforcement using data collection and retention until the Data Protection Directive has been agreed;

13. Recalls in this regard the EU-US TFTP Agreement, which, according to the Europol Joint

Supervisory Body assessment reports, allows for the bulk transfer of personal data and is therefore liable to be struck down by constitutional courts on grounds of failure to comply with the proportionality criteria of the ECHR;

14. Stresses that companies offering services to EU citizens are obliged to comply with EU law, especially EU data protection laws, and opposes the notion of corporate self-regulation when it comes to fundamental rights;

15. Regrets the fact that the Commission has dropped the former Article 42 of the leaked version of the Data Protection Regulation; calls on the Commission to clarify why it decided to do so; calls on the Council to follow Parliament's approach and reinsert such a provision;

16. Stresses that companies providing services to EU citizens and residents which fall under third-country jurisdiction should provide those users with a clear and distinguishable warning on the possibility of personal data being processed by law enforcement and intelligence following secret orders or injunctions;

17. Notes the initiatives by those internet-based companies that have proactively engaged in disclosing the identity of the public authorities which have sought and obtained access to user data; urges all other such companies to follow suit without delay;

18. Stresses the need for procedures allowing whistleblowers to unveil secret surveillance schemes without having to fear legal consequences; calls on the Member States, acting in coordination with the EEAS, to offer political asylum to Edward Snowden, who has had the courage to reveal this vast and systematic violation of fundamental rights, and for his application to be processed swiftly;

19. Calls on the EU to discuss with its US counterparts the issue of the data protection rules to be applied in bilateral relations and, in this context, to ensure that fundamental rights and the right to privacy and data protection are respected by both sides; calls on the Commission to use all the negotiating instruments available to ensure that this objective is achieved;

20. Criticises the systematic abuse of the concept of 'national security' to cover national economic interests or the political interests of those in power; condemns any use of this undefined notion as justification for spying on EU citizens and diplomats;

21. Stresses the need to set up a European equivalent of the mixed parliamentary-judicial control and inquiry committees on intelligence services that currently exist in some Member States;

22. Instructs its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter and to report back to plenary by the end of the year, on a basis including an assessment of the possible creation of a control and inquiry committee at EU level which would examine the cooperation of Member States' intelligence agencies and the use of EU citizens' personal data;

23. Instructs its President to forward this resolution to the Council, the Commission, the Council of Europe, the parliaments of the Member States, the US President, the US Congress and Senate, and the US Secretaries for Homeland Security and Justice.