EUROPEAN PARLIAMENT 2009 - 2014

Plenary sitting

1.7.2013 B7-0336/2013

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))

Rebecca Harms, Daniel Cohn-Bendit, Jan Philipp Albrecht, Judith Sargentini, Reinhard Bütikofer, Carl Schlyter, Yannick Jadot, Raül Romeva i Rueda, Ana Miranda, Bart Staes, Catherine Grèze, Malika Benarab-Attou
on behalf of the Verts/ALE Group

B7-0336/2013

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, the Charter of Fundamental Rights of the European Union, Articles 2, 6 and 7 of the Treaty on European Union (TEU), Article 16 of the Treaty on the Functioning of the European Union and the case law of Member States' constitutional courts, the European Court of Justice and the European Court of Human Rights,

– 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,

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

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

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

A. whereas reports in the international press have revealed evidence that, through programmes such as PRISM, the US authorities are accessing and processing on a large scale the personal data of EU citizens and residents using US online service providers;

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

C. whereas a full response from the US authorities is yet to be received, despite the discussions which took place at the EU-US Justice Ministerial meeting in Dublin on 14 June 2013;

D. whereas the transatlantic partnership between the EU and the US is based on respect for fundamental rights, the rule of law, and loyal and equal cooperation;

E. 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;

F. whereas the companies involved in the PRISM programme, as reported in the international press, are all parties to the Safe Harbour Agreement;

G. whereas the US has signed and ratified the Convention on Cybercrime with effect from 2007, thus making its principles part of US domestic law;

H. whereas the Convention on Cybercrime provides that all measures for the 'collection of evidence in electronic form' of any criminal offence (Article 14) must provide for the adequate protection of fundamental human rights, in particular those laid down in the ECHR (Article 8, Privacy), must ensure compliance with 'the principle of proportionality' and must be subject to safeguards that include, inter alia, judicial or other independent supervision, grounds justifying application, and limitation of the scope and duration of such procedures (Article 15);

I. whereas the EU-US Agreement on Mutual Legal Assistance, as ratified by the Union and the Congress, stipulates modalities for gathering and exchanging information, and requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another;

J. whereas the Commission has announced that an EU-US expert group will now be convened to discuss the PRISM issue from both the data protection and the security perspective;

K. whereas the international press has also reported on the alleged cooperation and involvement of EU Member States in the PRISM programme and other such programmes or their gaining access to the databases created;

L. whereas several Member States have similar surveillance programmes or are discussing such programmes;

M. whereas according to ECHR case law, any such programme has to be demonstrably proportionate and necessary in a democratic society; 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';

N. whereas data protection reform is under way at EU level, through the revision of Directive 95/46/EC and its replacement with the proposed general Data Protection Regulation and the Data Protection Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data; whereas the draft Data Protection Regulation 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; whereas this article disappeared after strong lobbying from the US administration, and whereas only a very weak recital remained;

O. whereas the Member States are bound to respect the fundamental values enshrined in Article 2 TEU and in the Charter of Fundamental Rights;

P. whereas reports in the international press have revealed that the US authorities have systematically bugged the EU representations to the US and to the UN, and have infiltrated their computer networks;

Q. whereas reports in the press have revealed that the UK Government Communications Headquarters (GCHQ) has tapped into more than 200 fibre-optic cables to obtain access to telephone conversations and internet traffic and stores all of their traffic for three days and the metadata for 30 days, 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;

R. whereas other Member States reportedly access transnational electronic communications without a regular warrant but on the basis of special courts, while data is shared with other countries (Sweden), and whereas others may enhance their surveillance capabilities (the Netherlands, Germany); whereas concerns have been expressed in other countries in relation to the interception powers of the secret services (Poland);

S. whereas Article 5(1) of the Directive on privacy and electronic communications

(2002/58/EC) obliges Member States to ensure the confidentiality of communications and the related traffic, and in particular to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data; whereas Article 15(1) of the directive allows exceptions to this prohibition only if they constitute a necessary, appropriate and proportionate measure within a democratic society;

T. whereas secret surveillance measures are often unknown to the public and whereas those who expose them may face serious consequences in terms of being subject to criminal prosecution;

1. Expresses serious concern over the PRISM and TEMPORA programmes and other such programmes which involve data collection, since, should the information available up to now be confirmed, this would entail a serious violation of the fundamental right to privacy and data protection of EU citizens and residents, as well as of the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, and the freedom to conduct business;

2. Calls on the US authorities to provide the EU, without undue delay, with full information on the PRISM programme and other such programmes involving data collection, as requested by Commissioner Reding in her letter of 10 June 2013 to Attorney General Eric Holder;

3. Stresses that any limitations of fundamental rights have to comply with the rule of law and have to be strictly proportionate, appropriate and necessary in a democratic society in accordance with the Charter of Fundamental Rights;

4. Demands that the transatlantic expert group, as announced by Commissioner Malmström and with the participation of Parliament, be granted an appropriate security clearance level and access to all appropriate documents, in order to be able to conduct its work properly and within a set deadline;

5. Calls on the Commission and the US administration to resume, without delay, the negotiations on the framework agreement on protection of personal data when transferred and processed for police and judicial cooperation purposes; calls on the Commission and the US administration to include special provisions on access by public authorities to personal data and information held by private entities for commercial purposes, and to ensure that EU citizens enjoy the same enforceable rights and protections as US citizens and residents;

6. Calls on the Commission to conduct a full review of the Safe Harbour Agreement in the light of the recent information, under Article 3 of the Agreement;

7. Expresses serious concern at the revelations relating to the alleged surveillance programmes run by Member States, either with the aid of the US National Security Agency or unilaterally;

8. Calls on the Member States to ensure that their respective laws and practices are in full conformity with the principles of necessity and proportionality, the ECHR and the related case law and, should they not be, to review them accordingly;

9. Calls on the Council, as a matter of urgency, to accelerate its work on the whole of the Data Protection Package, and specifically on the proposed Data Protection Directive;

10. Stresses that all companies offering services to EU citizens have to comply with EU law without exception, and are liable for any breaches;

11. Stresses that companies that fall under third-country jurisdiction should provide users located in the EU with a clear and distinguishable warning concerning the possibility of personal data being processed by law enforcement and intelligence following secret orders or injunctions;

12. Stresses that any laws establishing surveillance measures must be clearly drafted so as to indicate the categories of citizens targeted, the clear and precise purposes of the measure, the conditions of the interference, the rights of individuals, strict time limits for storage of data and destruction or erasure of the data after expiry of the time limits, as well as conditions for sharing data with third countries;

13. Strongly condemns the spying on EU representations as, should the information available until now be confirmed, it would imply a serious violation of the Vienna Convention on Diplomatic Relations, in addition to its potential impact on transatlantic relations;

14. Stresses the need for procedures allowing whistleblowers to unveil unlawful secret surveillance schemes without having to fear personal consequences; calls on the Member States to offer asylum to whistleblower Edward Snowden, in the spirit of the European Union Guidelines on Human Rights Defenders;

15. Calls on the Commission to ensure that EU data protection standards, and the negotiations on the current EU data protection package, are not undermined as a result of the Transatlantic Trade and Investment Partnership (TTIP) with the US, and to postpone the TTIP negotiations until the US has stopped its spying activities on EU institutions; requests the Commission, therefore, to cancel the first round of negotiations scheduled for Washington DC;

16. Calls on the Commission to immediately take out infringement proceedings under Article 259 TFEU against Member States whose surveillance measures are not compatible with EU law;

17. 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;

18. Stresses that these revelations seriously call into question trust in cloud computing and other information society services, particularly where the providers are subject to a third-country jurisdiction;

19. Notes that EU providers have reported a large increase in customer inquiries as a result of the reports about the PRISM programme;

20. Stresses that this could be turned into a competitive advantage for EU-based cloud computing and other information society services, provided there are strong data protection rules in place that also protect against access to data by third-country authorities and data-grabbing by Member States' intelligence services;

21. Calls on the Commission to revise its cloud computing strategy in light of the revelations and to set up a clear and consistent cloud computing initiative that addresses all these issues and promotes EU cloud initiatives that fully embody the protection of all civil liberties;

22. Calls for Parliament to carry out an in-depth inquiry into the matter, and for a report to be submitted to plenary by the end of the year, on the basis of effective competences to investigate, in particular, the measures taken by EU and Member State institutions;

23. Instructs its President to forward this resolution to the Commission, the Council, 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.