



EUROPEAN PARLIAMENT

2009 - 2014

---

*Plenary sitting*

---

**A7-0139/2014**

21.2.2014

## **REPORT**

on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

(2013/2188(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

**CONTENTS**

	<b>Page</b>
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION .....	3
EXPLANATORY STATEMENT.....	45
ANNEX I: LIST OF WORKING DOCUMENTS.....	52
ANNEX II: LIST OF HEARINGS AND EXPERTS .....	53
ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS.....	61
RESULT OF FINAL VOTE IN COMMITTEE .....	63

## MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs  
**(2013/2188(INI))**

*The European Parliament,*

- having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,
- having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,
- having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,
- having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,
- having regard to the European Convention on Human Rights, notably Articles 6, 8, 9, 10 and 13 thereof, and the protocols thereto,
- having regard to the Universal Declaration of Human Rights, notably Articles 7, 8, 10, 11, 12 and 14 thereof<sup>1</sup>,
- having regard to the International Covenant on Civil and Political Rights, notably Articles 14, 17, 18 and 19 thereof,
- having regard to the Council of Europe Convention on Data Protection (ETS No 108) and the Additional Protocol of 8 November 2001 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181),
- having regard to the Vienna Convention on Diplomatic Relations, notably Articles 24, 27 and 40 thereof,
- having regard to the Council of Europe Convention on Cybercrime (ETS No 185),
- having regard to the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, submitted on 17 May 2010<sup>2</sup>,
- having regard to the report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted on 17 April

---

<sup>1</sup> <http://www.un.org/en/documents/udhr/>

<sup>2</sup> <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

2013<sup>1</sup>,

- having regard to the Guidelines on human rights and the fight against terrorism adopted by the Committee of Ministers of the Council of Europe on 11 July 2002,
- having regard to the Declaration of Brussels of 1 October 2010, adopted at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States,
- having regard to Council of Europe Parliamentary Assembly Resolution No 1954 (2013) on national security and access to information,
- having regard to the report on the democratic oversight of the security services adopted by the Venice Commission on 11 June 2007<sup>2</sup>, and expecting with great interest the update thereof, due in spring 2014,
- having regard to the testimonies of the representatives of the oversight committees on intelligence of Belgium, the Netherlands, Denmark and Norway,
- having regard to the cases lodged before the French<sup>3</sup>, Polish and British<sup>4</sup> courts, as well as before the European Court of Human Rights<sup>5</sup>, in relation to systems of mass surveillance,
- having regard to the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, and in particular to Title III thereof<sup>6</sup>,
- having regard to Commission Decision 520/2000 of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,
- having regard to the Commission's assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)0196) and of 20 October 2004 (SEC(2004)1323),
- having regard to the Commission communication of 27 November 2013 (COM(2013)0847) on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU, and to the Commission communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)0846),
- having regard to its resolution of 5 July 2000 on the Draft Commission Decision on

---

<sup>1</sup> [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)

<sup>2</sup> [http://www.venice.coe.int/webforms/documents/CDL-AD\(2007\)016.aspx](http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx)

<sup>3</sup> La Fédération Internationale des Ligues des Droits de l'Homme and La Ligue française pour la défense des droits de l'Homme et du Citoyen v. X; Tribunal de Grande Instance of Paris.

<sup>4</sup> Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.

<sup>5</sup> Joint Application Under Article 34 of Big Brother Watch, Open Rights Group, English PEN and Dr Constanze Kurz (applicants) v. United Kingdom (respondent).

<sup>6</sup> OJ C 197, 12.7.2000, p. 1.

- the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, which took the view that the adequacy of the system could not be confirmed<sup>1</sup>, and to the Opinions of the Article 29 Working Party, more particularly Opinion 4/2000 of 16 May 2000<sup>2</sup>,
- having regard to the agreements between the United States of America and the European Union on the use and transfer of passenger name records (PNR agreement) of 2004, 2007<sup>3</sup> and 2012<sup>4</sup>,
  - having regard to the Joint Review of the implementation of the Agreement between the EU and the USA on the processing and transfer of passenger name records to the US Department of Homeland Security<sup>5</sup>, accompanying the report from the Commission to the European Parliament and to the Council on the joint review (COM(2013)0844),
  - having regard to the opinion of Advocate-General Cruz Villalón concluding that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks is as a whole incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union and that Article 6 thereof is incompatible with Articles 7 and 52(1) of the Charter<sup>6</sup>,
  - having regard to Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the 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 (TFTP)<sup>7</sup> and the accompanying declarations by the Commission and the Council,
  - having regard to the Agreement on mutual legal assistance between the European Union and the United States of America<sup>8</sup>,
  - having regard to the ongoing negotiations on an EU-US framework agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters (the ‘Umbrella agreement’),
  - having regard to Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted

---

<sup>1</sup> OJ C 121, 24.4.2001, p. 152.

<sup>2</sup> <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf>

<sup>3</sup> OJ L 204, 4.8.2007, p. 18.

<sup>4</sup> OJ L 215, 11.8.2012, p. 5.

<sup>5</sup> SEC(2013)0630, 27.11.2013.

<sup>6</sup> Opinion of Advocate General Cruz Villalón, 12 December 2013, Case C-293/12.

<sup>7</sup> OJ L 195, 27.7.2010, p. 3.

<sup>8</sup> OJ L 181, 19.7.2003, p. 34.

- by a third country, and actions based thereon or resulting therefrom<sup>1</sup>,
- having regard to the statement by the President of the Federative Republic of Brazil at the opening of the 68th session of the UN General Assembly on 24 September 2013 and to the work carried out by the Parliamentary Committee of Inquiry on Espionage established by the Federal Senate of Brazil,
  - having regard to the USA PATRIOT Act signed by President George W. Bush on 26 October 2001,
  - having regard to the Foreign Intelligence Surveillance Act (FISA) of 1978 and the FISA Amendments Act of 2008,
  - having regard to Executive Order No 12333, issued by the US President in 1981 and amended in 2008,
  - having regard to the Presidential Policy Directive (PPD-28) on Signals Intelligence Activities, issued by US President Barack Obama on 17 January 2014,
  - having regard to legislative proposals currently under examination in the US Congress including the draft US Freedom Act, the draft Intelligence Oversight and Surveillance Reform Act, and others,
  - having regard to the reviews conducted by the Privacy and Civil Liberties Oversight Board, the US National Security Council and the President’s Review Group on Intelligence and Communications Technology, particularly the report by the latter of 12 December 2013 entitled ‘Liberty and Security in a Changing World’,
  - having regard to the ruling of the United States District Court for the District of Columbia, *Klayman et al. v Obama et al.*, Civil Action No 13-0851 of 16 December 2013, and to the ruling of the United States District Court for the Southern District of New York, *ACLU et al. v James R. Clapper et al.*, Civil Action No 13-3994 of 11 June 2013,
  - having regard to the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection of 27 November 2013<sup>2</sup>,
  - having regard to its resolutions of 5 September 2001 and 7 November 2002 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),
  - having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU<sup>3</sup>,
  - having regard to its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their

---

<sup>1</sup> OJ L 309, 29.11.1996, p.1.

<sup>2</sup> Council document 16987/13.

<sup>3</sup> Texts adopted, P7\_TA(2013)0203.

- impact on EU citizens, whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter<sup>1</sup>,
- having regard to working document 1 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights,
  - having regard to working document 3 on the relation between the surveillance practices in the EU and the US and the EU data protection provisions,
  - having regard to working document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation,
  - having regard to working document 5 on democratic oversight of Member State intelligence services and of EU intelligence bodies,
  - having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken<sup>2</sup>,
  - having regard to its resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance<sup>3</sup>,
  - having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing<sup>4</sup>,
  - having regard to the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy<sup>5</sup>,
  - having regard to Annex VIII of its Rules of Procedure,
  - having regard to Rule 48 of its Rules of Procedure,
  - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A7-0139/2014),

### ***The impact of mass surveillance***

- A. whereas data protection and privacy are fundamental rights; whereas security measures, including counterterrorism measures, must therefore be pursued through the rule of law and must be subject to fundamental rights obligations, including those relating to privacy and data protection;
- B. whereas the ties between Europe and the United States of America are based on the

---

<sup>1</sup> Texts adopted, P7\_TA(2013)0322.

<sup>2</sup> Texts adopted, P7\_TA(2013)0444.

<sup>3</sup> Texts adopted, P7\_TA(2013)0449.

<sup>4</sup> Texts adopted, P7\_TA(2013)0535.

<sup>5</sup> OJ C 353 E, 3.12.2013, p.156.

spirit and principles of democracy, the rule of law, liberty, justice and solidarity;

- C. whereas cooperation between the US and the European Union and its Member States in counter-terrorism remains vital for the security and safety of both partners;
- D. whereas mutual trust and understanding are key factors in the transatlantic dialogue and partnership;
- E. whereas following 11 September 2001, the fight against terrorism became one of the top priorities of most governments; whereas the revelations based on documents leaked by the former NSA contractor Edward Snowden put political leaders under the obligation to address the challenges of overseeing and controlling intelligence agencies in surveillance activities and assessing the impact of their activities on fundamental rights and the rule of law in a democratic society;
- F. whereas the revelations since June 2013 have caused numerous concerns within the EU as to:
- the extent of the surveillance systems revealed both in the US and in EU Member States;
  - the violation of EU legal standards, fundamental rights and data protection standards;
  - the degree of trust between the EU and the US as transatlantic partners;
  - the degree of cooperation and involvement of certain EU Member States with US surveillance programmes or equivalent programmes at national level as unveiled by the media;
  - the lack of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities;
  - the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds;
  - the undermining of press freedom and of communications of members of professions with a confidentiality privilege, including lawyers and doctors;
  - the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies;
  - the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillance;
  - the threats to privacy in a digital era;
- G. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European institutions and Member States' governments, national parliaments and judicial authorities;



- H. whereas the US authorities have denied some of the information revealed but have not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in certain EU Member States; whereas EU governments and parliaments too often remain silent and fail to launch adequate investigations;
- I. whereas President Obama has recently announced a reform of the NSA and its surveillance programmes;
- J. whereas in comparison to actions taken both by EU institutions and by certain EU Member States, the European Parliament has taken very seriously its obligation to shed light on the revelations on the indiscriminate practices of mass surveillance of EU citizens and, by means of its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens, instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter;
- K. whereas it is the duty of the European institutions to ensure that EU law is fully implemented for the benefit of European citizens and that the legal force of the EU Treaties is not undermined by a dismissive acceptance of extraterritorial effects of third countries' standards or actions;

***Developments in the US on reform of intelligence***

- L. whereas the District Court for the District of Columbia, in its Decision of 16 December 2013, has ruled that the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution<sup>1</sup> ; whereas, however the District Court for the Southern District of New York ruled in its Decision of 27 December 2013 that this collection was lawful;
- M. whereas a Decision of the District Court for the Eastern District of Michigan has ruled that the Fourth Amendment requires reasonableness in all searches, prior warrants for any reasonable search, warrants based upon prior-existing probable cause, as well as particularity as to persons, place and things and the interposition of a neutral magistrate between executive branch enforcement officers and citizens<sup>2</sup>;
- N. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 46 recommendations to the President of the United States; whereas the recommendations stress the need simultaneously to protect national security and personal privacy and civil liberties; whereas in this regard it invites the US Government: to end bulk collection of phone records of US persons under Section 215 of the USA PATRIOT Act as soon as practicable; to undertake a thorough review of the NSA and the US intelligence legal framework in order to ensure respect for the right to privacy; to end efforts to subvert or make vulnerable commercial software (backdoors and malware); to increase the use of encryption, particularly in the case of data in transit, and not to undermine efforts to create encryption standards; to create a Public Interest Advocate to represent privacy

---

<sup>1</sup> Klayman et al. v Obama et al., Civil Action No 13-0851, 16 December 2013.

<sup>2</sup> ACLU v. NSA No 06-CV-10204, 17 August 2006.

and civil liberties before the Foreign Intelligence Surveillance Court; to confer on the Privacy and Civil Liberties Oversight Board the power to oversee Intelligence Community activities for foreign intelligence purposes, and not only for counterterrorism purposes; and to receive whistleblowers' complaints, to use Mutual Legal Assistance Treaties to obtain electronic communications, and not to use surveillance to steal industry or trade secrets;

- O. whereas, according to an open memorandum submitted to President Obama by Former NSA Senior Executives/Veteran Intelligence Professionals for Sanity (VIPS) on 7 January 2014,<sup>1</sup> the massive collection of data does not enhance the ability to prevent future terrorist attacks; whereas the authors stress that mass surveillance conducted by the NSA has resulted in the prevention of zero attacks and that billions of dollars have been spent on programmes which are less effective and vastly more intrusive on citizens' privacy than an in-house technology called THINTHREAD that was created in 2001;
- P. whereas in respect of intelligence activities concerning non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental principle of respect for privacy and human dignity as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; whereas they do not recommend granting non-US persons the same rights and protections as US persons;
- Q. whereas in his Presidential Policy Directive on Signals Intelligence Activities of 17 January 2014 and the related speech, US President Barack Obama stated that mass electronic surveillance is necessary for the United States to protect its national security, its citizens and the citizens of US allies and partners, as well as to advance its foreign policy interests; whereas this policy directive contains certain principles regarding the collection, use and sharing of signals intelligence and extends certain safeguards to non-US persons, partly providing for treatment equivalent to that enjoyed by US citizens, including safeguards for the personal information of all individuals regardless of their nationality or residence; whereas, however, President Obama did not call for any concrete proposals, particularly regarding the prohibition of mass surveillance activities and the introduction of administrative and judicial redress for non-US persons;

### ***Legal framework***

#### *Fundamental rights*

- R. whereas the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection provides for an overview of the legal situation in the US, but has failed to establish the facts about US surveillance programmes; whereas no information has been made available about the so-called 'second track' Working Group, under which Member States discuss bilaterally with the US authorities matters related to national security;

---

<sup>1</sup> <http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong>.

- S. whereas fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy; whereas mass surveillance of human beings is incompatible with these cornerstones;
- T. whereas in all Member States the law protects from disclosure information communicated in confidence between lawyer and client, a principle which has been recognised by the European Court of Justice<sup>1</sup>;
- U. whereas in its resolution of 23 October 2013 on organised crime, corruption and money laundering Parliament called on the Commission to submit a legislative proposal establishing an effective and comprehensive European whistleblower protection programme in order to protect EU financial interests and furthermore conduct an examination on whether such future legislation should also cover other fields of Union competence;

*Union competences in the field of security*

- V. whereas according to Article 67(3) TFEU the EU ‘shall endeavour to ensure a high level of security’; whereas the provisions of the Treaty (in particular Article 4(2) TEU, Article 72 TFEU and Article 73 TFEU) imply that the EU possesses certain competences on matters relating to the collective external security of the Union; whereas the EU has competence in matters of internal security (Article 4(j) TFEU) and has exercised this competence by deciding on a number of legislative instruments and concluding international agreements (PNR, TFTP) aimed at fighting serious crime and terrorism, and by setting up an internal security strategy and agencies working in this field;
- W. whereas the Treaty on the Functioning of the European Union states that ‘it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security’ (Article 73 TFEU);
- X. whereas Article 276 TFEU states that ‘in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security’;
- Y. whereas the concepts of ‘national security’, ‘internal security’, ‘internal security of the

---

<sup>1</sup> Judgement of 18 May 1982 in Case C-155/79, AM & S Europe Limited v Commission of the European Communities

EU' and 'international security' overlap; whereas the Vienna Convention on the Law of Treaties, the principle of sincere cooperation among EU Member States and the human rights law principle of interpreting any exemptions narrowly point towards a restrictive interpretation of the notion of 'national security' and require that Member States refrain from encroaching upon EU competences;

- Z. whereas the European Treaties confer on the European Commission the role of the 'Guardian of the Treaties', and it is therefore the legal responsibility of the Commission to investigate any potential breaches of EU law;
- AA. whereas, in accordance with Article 6 TEU, referring to the EU Charter of Fundamental Rights and the ECHR, Member States' agencies and even private parties acting in the field of national security also have to respect the rights enshrined therein, be they of their own citizens or of citizens of other states;

#### *Extraterritoriality*

- AB. whereas the extraterritorial application by a third country of its laws, regulations and other legislative or executive instruments in situations falling under the jurisdiction of the EU or its Member States may impact on the established legal order and the rule of law, or even violate international or EU law, including the rights of natural and legal persons, taking into account the extent and the declared or actual aim of such an application; whereas, in these circumstances, it is necessary to take action at Union level to ensure that the EU values enshrined in Article 2 TEU, the Charter of Fundamental Rights, the ECHR referring to fundamental rights, democracy and the rule of law, and the rights of natural and legal persons as enshrined in secondary legislation applying these fundamental principles, are respected within the EU, for example by removing, neutralising, blocking or otherwise countering the effects of the foreign legislation concerned;

#### *International transfers of data*

- AC. whereas the transfer of personal data by EU institutions, bodies, offices or agencies or by the Member States to the US for law enforcement purposes in the absence of adequate safeguards and protections for the respect of the fundamental rights of EU citizens, in particular the rights to privacy and the protection of personal data, would make that EU institution, body, office or agency or that Member State liable, under Article 340 TFEU or the established case law of the CJEU<sup>1</sup>, for breach of EU law – which includes any violation of the fundamental rights enshrined in the EU Charter;
- AD. whereas the transfer of data is not geographically limited, and, especially in a context of increasing globalisation and worldwide communication, the EU legislator is confronted with new challenges in terms of protecting personal data and communications; whereas it is therefore of the utmost importance to foster legal frameworks on common standards;
- AE. whereas the mass collection of personal data for commercial purposes and in the fight

---

<sup>1</sup> See notably Joined Cases C-6/90 and C-9/90, *Francovich and others v. Italy*, judgment of 28 May 1991.

against terror and serious transnational crime puts at risk the personal data and privacy rights of EU citizens;

*Transfers to the US based on the US Safe Harbour*

- AF. whereas the US data protection legal framework does not ensure an adequate level of protection for EU citizens;
- AG. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 520/2000, has declared the adequacy of the protection provided by the Safe Harbour privacy principles and the related FAQs issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the US that have joined the Safe Harbour;
- AH. whereas in its resolution of 5 July 2000 Parliament expressed doubts and concerns as to the adequacy of the Safe Harbour, and called on the Commission to review the decision in good time, in the light of experience and of any legislative developments;
- AI. whereas in Parliament's working document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation of 12 December 2013, the rapporteurs expressed doubts and concerns as to the adequacy of Safe Harbour and called on the Commission to repeal the decision on the adequacy of Safe Harbour and to find new legal solutions;
- AJ. whereas Commission Decision 520/2000 stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;
- AK. whereas Commission Decision 520/2000 also states that where evidence has been provided that anybody responsible for ensuring compliance with the principles is not effectively fulfilling their role, the Commission must inform the US Department of Commerce and, if necessary, present measures with a view to reversing or suspending the Decision or limiting its scope;
- AL. whereas in its first two reports on the implementation of the Safe Harbour, published in 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made a number of recommendations to the US authorities with a view to rectifying those deficiencies;
- AM. whereas in its third implementation report, of 27 November 2013, nine years after the second report and without any of the deficiencies recognised in that report having been rectified, the Commission identified further wide-ranging weaknesses and shortcomings in the Safe Harbour and concluded that the current implementation could not be maintained; whereas the Commission has stressed that wide-ranging access by US intelligence agencies to data transferred to the US by Safe

Harbour-certified entities raises additional serious questions as to the continuity of protection of the data of EU data subjects; whereas the Commission addressed 13 recommendations to the US authorities and undertook to identify by summer 2014, together with the US authorities, remedies to be implemented as soon as possible, forming the basis for a full review of the functioning of the Safe Harbour principles;

- AN. whereas on 28-31 October 2013 a delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) met in Washington D.C. with the US Department of Commerce and the US Federal Trade Commission; whereas the Department of Commerce acknowledged the existence of organisations having self-certified adherence to Safe Harbour Principles but clearly showing a 'not-current status', meaning that the company does not fulfil Safe Harbour requirements although continuing to receive personal data from the EU; whereas the Federal Trade Commission admitted that the Safe Harbour should be reviewed in order to improve it, particularly with regard to complaints and alternative dispute resolution systems;
- AO. whereas Safe Harbour Principles may be limited 'to the extent necessary to meet national security, public interest, or law enforcement requirements'; whereas, as an exception to a fundamental right, such an exception must always be interpreted restrictively and be limited to what is necessary and proportionate in a democratic society, and the law must clearly establish the conditions and safeguards to make this limitation legitimate; whereas the scope of application of such exception should have been clarified by the US and the EU, notably by the Commission, to avoid any interpretation or implementation that nullifies in substance the fundamental right to privacy and data protection, among others; whereas, consequently, such an exception should not be used in a way that undermines or nullifies the protection afforded by Charter of Fundamental Rights, the ECHR, the EU data protection law and the Safe Harbour principles; insists that if the national security exception is invoked, it must be specified under which national law;
- AP. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on trust as regards US organisations acting in the EU; whereas this is further exacerbated by the lack of judicial and administrative redress for EU citizens under US law, particularly in cases of surveillance activities for intelligence purposes;

***Transfers to third countries with the adequacy decision***

- AQ. whereas according to the information revealed and to the findings of the inquiry conducted by the LIBE Committee, the national security agencies of New Zealand, Canada and Australia have been involved on a large scale in mass surveillance of electronic communications and have actively cooperated with the US under the so-called 'Five Eyes' programme, and may have exchanged with each other personal data of EU citizens transferred from the EU;
- AR. whereas Commission Decisions 2013/65<sup>1</sup> and 2/2002 of 20 December 2001<sup>2</sup> have

---

<sup>1</sup> OJ L 28, 30.1.2013, p. 12.

<sup>2</sup> OJ L 2, 4.1.2002, p. 13.

declared the levels of protection ensured by, respectively, the New Zealand Privacy Act and the Canadian Personal Information Protection and Electronic Documents Act to be adequate ; whereas the aforementioned revelations also seriously affect trust in the legal systems of these countries as regards the continuity of protection afforded to EU citizens; whereas the Commission has not examined this aspect;

*Transfers based on contractual clauses and other instruments*

- AS. whereas Directive 95/46/EC provides that international transfers to a third country may also take place by means of specific instruments whereby the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights;
- AT. whereas such safeguards may in particular result from appropriate contractual clauses;
- AU. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive, and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;
- AV. whereas the Commission Decisions establishing the standard contractual clauses stipulate that the competent authorities in Member States may exercise their existing powers to suspend data flows where it is established that the law to which the data importer or a sub-processor is subject imposes upon them requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or where there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects;
- AW. whereas national data protection authorities have developed binding corporate rules (BCRs) in order to facilitate international transfers within a multinational corporation with adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; whereas before being used, BCRs need to be authorised by the Member States' competent authorities after the latter have assessed compliance with Union data protection law; whereas BCRs for data processors have been rejected in the LIBE Committee report on the General Data Protection Regulation, as they would leave the data controller and the data subject without any control over the jurisdiction in which their data is processed;
- AX. whereas the European Parliament, given its competence stipulated by Article 218 TFEU, has the responsibility to continuously monitor the value of international agreements it has given its consent to;

*Transfers based on TFTP and PNR agreements*

- AY. whereas in its resolution of 23 October 2013 Parliament expressed serious concerns over the revelations concerning the NSA's activities as regards direct access to financial payments messages and related data, which would constitute a clear breach of the TFTP Agreement, and in particular Article 1 thereof;
- AZ. whereas terrorist finance tracking is an essential tool in the fight against terrorism financing and serious crime, allowing counterterrorism investigators to discover links between targets of investigation and other potential suspects connected with wider terrorist networks suspected of financing terrorism;
- BA. whereas Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations; whereas the Commission has done neither;
- BB. whereas following the allegations published by the media, the Commission decided to open consultations with the US pursuant to Article 19 of the TFTP Agreement; whereas on 27 November 2013 Commissioner Malmström informed the LIBE Committee that, after meeting US authorities and in view of the replies given by the US authorities in their letters and during their meetings, the Commission had decided not to pursue the consultations on the grounds that there were no elements showing that the US Government has acted in a manner contrary to the provisions of the Agreement, and that the US has provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP agreement; whereas it is not clear whether the US authorities have circumvented the Agreement by accessing such data through other means, as indicated in the letter of 18 September 2013 from the US authorities<sup>1</sup>;
- BC. whereas during its visit to Washington of 28-31 October 2013 the LIBE delegation met with the US Department of the Treasury; whereas the US Treasury stated that since the entry into force of the TFTP Agreement it had not had access to data from SWIFT in the EU except within the framework of the TFTP; whereas the US Treasury refused to comment on whether SWIFT data would have been accessed outside TFTP by any other US government body or department or whether the US administration was aware of NSA mass surveillance activities; whereas on 18 December 2013 Mr Glenn Greenwald stated before the inquiry held by the LIBE Committee that the NSA and GCHQ had targeted SWIFT networks;
- BD. whereas the Belgian and Netherlands data protection authorities decided on 13 November 2013 to conduct a joint investigation into the security of SWIFT's payment networks in order to ascertain whether third parties could gain unauthorised or unlawful access to European citizens' bank data<sup>2</sup>;

---

<sup>1</sup> The letter states that 'the US government seeks and obtains financial information ... [which] is collected through regulatory, law enforcement, diplomatic and intelligence channels, as well as through exchanges with foreign partners' and that 'the US Government is using the TFTP to obtain SWIFT data that we do not obtain from other sources'.

<sup>2</sup> <http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de->



- BE. whereas according to the Joint Review of the EU-US PNR agreement, the US Department of Homeland Security (DHS) made 23 disclosures of PNR data to the NSA on a case-by-case basis in support of counterterrorism cases, in a manner consistent with the specific terms of the Agreement;
- BF. whereas the Joint Review fails to 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, and constitutional protections are only granted to US persons; whereas this lack of judicial or administrative rights nullifies the protections for EU citizens laid down in the existing PNR agreement;

*Transfers based on the EU-US Mutual Legal Assistance Agreement in criminal matters*

- BG. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003<sup>1</sup> entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and the US to combat crime in a more effective way, having due regard for the rights of individuals and the rule of law;

*Framework agreement on data protection in the field of police and judicial cooperation ('umbrella agreement')*

- BH. whereas the purpose of this general agreement is to establish the legal framework for all transfers of personal data between the EU and US for the sole purposes of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters; whereas negotiations were authorised by the Council on 2 December 2010; whereas this agreement is of the utmost importance and would act as the basis to facilitate data transfer in the context of police and judicial cooperation and in criminal matters;
- BI. whereas this agreement should provide for clear and precise and legally binding data-processing principles, and should in particular recognise EU citizens' right to judicial access to and rectification and erasure of their personal data in the US, as well as the right to an efficient administrative and judicial redress mechanism for EU citizens in the US and independent oversight of the data-processing activities;
- BJ. whereas in its communication of 27 November 2013 the Commission indicated that the 'umbrella agreement' should result in a high level of protection for citizens on both sides of the Atlantic and should strengthen the trust of Europeans in EU-US data exchanges, providing a basis on which to develop EU-US security cooperation and partnership further;
- BK. whereas negotiations on the agreement have not progressed because of the US Government's persistent position of refusing recognition of effective rights of administrative and judicial redress to EU citizens and because of the intention of providing broad derogations to the data protection principles contained in the

---

[contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la](#)

<sup>1</sup> OJ L 181, 19.7.2003, p. 25.

agreement, such as purpose limitation, data retention or onward transfers either domestically or abroad;

### ***Data protection reform***

- BL. whereas the EU data protection legal framework is currently being reviewed in order to establish a comprehensive, consistent, modern and robust system for all data-processing activities in the Union; whereas in January 2012 the Commission presented a package of legislative proposals: a General Data Protection Regulation<sup>1</sup>, which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive<sup>2</sup> which will lay down a harmonised framework for all data processing activities by law enforcement authorities for law enforcement purposes and will reduce the current divergences among national laws;
- BM. whereas on 21 October 2013 the LIBE Committee adopted its legislative reports on the two proposals and a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term;
- BN. whereas, although the European Council of 24/25 October 2013 called for the timely adoption of a strong EU General Data Protection framework in order to foster the trust of citizens and businesses in the digital economy, after two years of deliberations the Council has still been unable to arrive at a general approach on the General Data Protection Regulation and the Directive<sup>3</sup>;

### ***IT security and cloud computing***

- BO. whereas Parliament's resolution of 10 December 2013<sup>4</sup> emphasises the economic potential of 'cloud computing' business for growth and employment; whereas the overall economic value of the cloud market is forecast to be worth USD 207 billion a year by 2016, or twice its value in 2012;
- BP. whereas the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context; whereas Union data protection law, since it is technologically neutral, already applies fully to cloud computing services operating in the EU;
- BQ. whereas mass surveillance activities give intelligence agencies access to personal data stored or otherwise processed by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored or otherwise processed in servers located on EU soil by tapping into the internal networks of Yahoo and Google; whereas such activities constitute a violation of international obligations and of European fundamental rights standards including the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, freedom of assembly and association and the freedom to conduct business; whereas it

---

<sup>1</sup> COM(2012)0011, 25.1.2012.

<sup>2</sup> COM(2012)0010, 25.1.2012.

<sup>3</sup> [http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/139197.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf)

<sup>4</sup> A7-0353/2013 - PE506.114v2.00.

is not excluded that information stored in cloud services by Member States' public authorities or undertakings and institutions has also been accessed by intelligence authorities;

- BR. whereas US intelligence agencies have a policy of systematically undermining cryptographic protocols and products in order to be able to intercept even encrypted communication; whereas the US National Security Agency has collected vast numbers of so called 'zero-day exploits' – IT security vulnerabilities that are not yet known to the public or the product vendor; whereas such activities massively undermine global efforts to improve IT security;
- BS. whereas the fact that intelligence agencies have accessed personal data of users of online services has severely distorted the trust of citizens in such services, and therefore has an adverse effect on businesses investing in the development of new services using 'Big Data' and new applications such as the 'Internet of Things';
- BT. whereas IT vendors often deliver products that have not been properly tested for IT security or that even sometimes have backdoors implanted purposefully by the vendor; whereas the lack of liability rules for software vendors has led to such a situation, which is in turn exploited by intelligence agencies but also leaves open the risk of attacks by other entities;
- BU. whereas it is essential for companies providing such new services and applications to respect the data protection rules and privacy of the data subjects whose data are collected, processed and analysed, in order to maintain a high level of trust among citizens;

#### ***Democratic oversight of intelligence services***

- BV. whereas intelligence services in democratic societies are given special powers and capabilities to protect fundamental rights, democracy and the rule of law, citizens' rights and the State against internal and external threats, and are subject to democratic accountability and judicial oversight; whereas they are given special powers and capabilities only to this end; whereas these powers should be used within the legal limits imposed by fundamental rights, democracy and the rule of law and their application should be strictly scrutinised, as otherwise they lose legitimacy and risk undermining democracy;
- BW. whereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing modi operandi or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society;
- BX. whereas most of the existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid political and technological developments over the last decade that have led to increased international intelligence cooperation, also through the large scale exchange of

- personal data, and often blurring the line between intelligence and law enforcement activities;
- BY. whereas democratic oversight of intelligence activities is still only conducted at national level, despite the increase in exchange of information between EU Member States and between Member States and third countries; whereas there is an increasing gap between the level of international cooperation on the one hand and oversight capacities limited to the national level on the other, which results in insufficient and ineffective democratic scrutiny;
- BZ. whereas national oversight bodies often do not have full access to intelligence received from a foreign intelligence agency, which can lead to gaps in which international information exchanges can take place without adequate review; whereas this problem is further aggravated by the so-called ‘third party rule’ or the principle of ‘originator control’, which has been designed to enable originators to maintain control over the further dissemination of their sensitive information, but is unfortunately often interpreted as applying also to the recipient services’ oversight;
- CA. whereas private and public transparency reform initiatives are key to ensuring public trust in the activities of intelligence agencies; whereas legal systems should not prevent companies from disclosing to the public information about how they handle all types of government requests and court orders for access to user data, including the possibility of disclosing aggregate information on the number of requests and orders approved and rejected;

### ***Main findings***

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States’ intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner;
2. Points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted ‘man-in-the-middle attacks’ on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme);
3. Notes the allegations of ‘hacking’ or tapping into the Belgacom systems by the UK intelligence agency GCHQ; notes the statements by Belgacom that it could neither

confirm nor deny that EU institutions were targeted or affected, and that the malware used was extremely complex and its development and use would require extensive financial and staffing resources that would not be available to private entities or hackers;

4. Emphasises that trust has been profoundly shaken: trust between the two transatlantic partners, trust between citizens and their governments, trust in the functioning of democratic institutions on both sides of the Atlantic, trust in the respect of the rule of law, and trust in the security of IT services and communication; believes that in order to rebuild trust in all these dimensions, an immediate and comprehensive response plan comprising a series of actions which are subject to public scrutiny is needed;
5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society;
6. Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection;
7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled;
8. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Titles I and VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union, as well as the principle that Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';
9. Notes that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances or for democratic accountability;
10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail

illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws;

11. Considers it crucial that the professional confidentiality privilege of lawyers, journalists, doctors and other regulated professions is safeguarded against mass surveillance activities; stresses, in particular, that any uncertainty about the confidentiality of communications between lawyers and their clients could negatively impact on EU citizens' right of access to legal advice and access to justice and the right to a fair trial;
12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in this regard the decision of the German Federal Constitutional Court<sup>1</sup> on the prohibition of the use of preventive dragnets ('präventive Rasterfahndung') unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measures;
13. Is convinced that secret laws and courts violate the rule of law; points out that any judgment of a court or tribunal and any decision of an administrative authority of a non-EU state authorising, directly or indirectly, the transfer of personal data, may not be recognised or enforced in any manner unless there is a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State and a prior authorisation by the competent supervisory authority; recalls that any judgment of a secret court or tribunal and any decision of an administrative authority of a non-EU state secretly authorising, directly or indirectly, surveillance activities shall not be recognised or enforced;
14. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data; considers that the scale of this problem is unprecedented; notes that this may create a situation where infrastructure for the mass collection and processing of data could be misused in cases of change of political regime;
15. Notes that there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from attacks by well-equipped intruders ('no 100 % IT security'); notes that in order to achieve maximum IT security, Europeans need to be willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance in the field of IT;

---

<sup>1</sup> No 1 BvR 518/02 of 4 April 2006.

16. Strongly rejects the notion that all issues related to mass surveillance programmes are purely a matter of national security and therefore the sole competence of Member States; reiterates that Member States must fully respect EU law and the ECHR while acting to ensure their national security; recalls a recent ruling of the Court of Justice according to which ‘although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable’<sup>1</sup>; recalls further that the protection of the privacy of all EU citizens is at stake, as are the security and reliability of all EU communication networks; believes, therefore, that discussion and action at EU level are not only legitimate, but also a matter of EU autonomy;
17. Commends the current discussions, inquiries and reviews concerning the subject of this inquiry in several parts of the world, including through the support of civil society; points to the Global Government Surveillance Reform signed up to by the world's leading technology companies calling for sweeping changes to national surveillance laws, including an international ban on bulk collection of data, to help preserve the public's trust in the internet and in their businesses; points to the calls made by hundreds of leading academics<sup>2</sup>, civil society organisations<sup>3</sup> and 562 international authors, including five Nobel laureates, for an end to mass surveillance; notes with great interest the recommendations published recently by the US President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court<sup>4</sup>; strongly urges governments to take these calls and recommendations fully into account and to overhaul their national frameworks for their intelligence services in order to implement appropriate safeguards and oversight;
18. Commends the institutions and experts who have contributed to this Inquiry; deplors the fact that several Member States’ authorities have declined to cooperate with the inquiry the European Parliament has been conducting on behalf of citizens; welcomes the openness of several Members of Congress and of national parliaments;
19. Is aware that in such a limited timeframe it has been possible to conduct only a preliminary investigation of all the issues at stake since July 2013; recognises both the scale of the revelations involved and their ongoing nature; adopts, therefore, a forward-planning approach consisting in a set of specific proposals and a mechanism for follow-up action in the next parliamentary term, ensuring the findings remain high on the EU political agenda;
20. Intends to request strong political undertakings from the new Commission which will be designated after the May 2014 European elections to the effect that it will implement the proposals and recommendations of this Inquiry; expects an appropriate level of commitment from the candidates in the upcoming parliamentary hearings for

---

<sup>1</sup> Judgement in Case C-300/11, ZZ v Secretary of State for the Home Department, 4 June 2013.

<sup>2</sup> [www.academicsagainstsurveillance.net](http://www.academicsagainstsurveillance.net).

<sup>3</sup> [www.stopspyingonus.com](http://www.stopspyingonus.com) and [www.en.necessaryandproportionate.org](http://www.en.necessaryandproportionate.org).

<sup>4</sup> <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf>.

the new Commissioners;

### ***Recommendations***

21. Calls on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities;
22. Calls on the EU Member States, and in particular those participating in the so-called '9-eyes' and '14-eyes' programmes<sup>1</sup>, to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, including by reference to the UN compilation of good practices and the recommendations of the Venice Commission, and that they are in line with the standards of the European Convention on Human Rights and comply with Member States' fundamental rights obligations, in particular as regards data protection, privacy, and the presumption of innocence;
23. Calls on all EU Member States and in particular, with regard to its Resolution of 4 July 2013 and Inquiry Hearings, the United Kingdom, France, Germany, Sweden, the Netherlands and Poland to ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and European Union data protection legislation; calls on these Member States to clarify the allegations of mass surveillance activities, including mass surveillance of cross border telecommunications, untargeted surveillance on cable-bound communications, potential agreements between intelligence services and telecommunication companies as regards access and exchange of personal data and access to transatlantic cables, US intelligence personnel and equipment on EU territory without oversight on surveillance operations, and their compatibility with EU legislation; invites the national parliaments of those countries to intensify cooperation of their intelligence oversight bodies at European level;
24. Calls on the United Kingdom, in particular, given the extensive media reports referring to mass surveillance by the intelligence service GCHQ, to revise its current legal framework, which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000;
25. Takes note of the review of the Dutch Intelligence and Security Act 2002 (report by the Dessens Commission of 2 December 2013); supports those recommendations of the review commission which aim to strengthen the transparency, control and oversight of the Dutch intelligence services; calls on the Netherlands to refrain from extending the powers of the intelligence services in such a way as to enable untargeted and large-scale surveillance also to be performed on cable-bound communications of

---

<sup>1</sup> The '9-eyes programme' comprises the US, the UK, Canada, Australia, New Zealand, Denmark, France, Norway and the Netherlands; the '14-eyes programme' includes those countries and also Germany, Belgium, Italy, Spain and Sweden.



innocent citizens, especially given the fact that one of the biggest Internet Exchange Points in the world is located in Amsterdam (AMS-IX); calls for caution in defining the mandate and capabilities of the new Joint Sigint Cyber Unit, as well as for caution regarding the presence and operation of US intelligence personnel on Dutch territory;

26. Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of human rights under the TEU, the ECHR and the EU Charter of Fundamental Rights;
27. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;
28. Invites the Secretary-General of the Council of Europe to launch the Article 52 procedure according to which 'on receipt of a request from the Secretary-General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention';
29. Calls on Member States to take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on Member States to make use of all available international measures to defend EU citizens' fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of the International Covenant on Civil and Political Rights (ICCPR);
30. Calls on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens, and to sign the Optional Protocol allowing for complaints by individuals under the ICCPR;
31. Welcomes, in this regard, the remarks made and the Presidential Policy Directive issued by US President Obama on 17 January 2014, as a step towards limiting authorisation of the use of surveillance and data processing to national security purposes and towards equal treatment of all individuals' personal information, regardless of their nationality or residence, by the US intelligence community; awaits, however, in the context of the EU-US relationship, further specific steps which will, most importantly, strengthen trust in transatlantic data transfers and provide for binding guarantees for enforceable privacy rights of EU citizens, as outlined in detail in this report;
32. Stresses its serious concerns in relation to the work within the Council of Europe's

Cybercrime Convention Committee on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 (Budapest Convention) on transborder access to stored computer data with consent or where publicly available, and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality because it could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, and in particular Council of Europe Convention 108;

33. Calls on the Commission to carry out, before July 2014, an assessment of the applicability of Regulation (EC) No 2271/96 to cases of conflict of laws on transfers of personal data;
34. Calls on the Fundamental Rights Agency to undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices;

### ***International transfers of data***

#### *US data protection legal framework and US Safe Harbour*

35. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by the US NSA are companies that have self-certified their adherence to the Safe Harbour, and that the Safe Harbour is the legal instrument used for the transfer of EU personal data to the US (examples being Google, Microsoft, Yahoo!, Facebook, Apple and LinkedIn); expresses its concerns that these organisations have not encrypted information and communications flowing between their data centres, thereby enabling intelligence services to intercept information; welcomes the subsequent statements by some US companies that they will accelerate plans to implement encryption of data flows between their global data centres;
36. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not meet the criteria for derogation under ‘national security’;
37. Takes the view that, as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out under other instruments, such as contractual clauses or BCRs, provided these instruments set out specific safeguards and protections and are not circumvented by other legal frameworks;
38. Takes the view that the Commission has failed to act to remedy the well-known deficiencies of the current implementation of Safe Harbour;

39. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce; calls on the US authorities, therefore, to put forward a proposal for a new framework for transfers of personal data from the EU to the US which meets Union law data protection requirements and provides for the required adequate level of protection;
40. Calls on Member States' competent authorities, in particular the data protection authorities, to make use of their existing powers and immediately suspend data flows to any organisation that has self-certified its adherence to the US Safe Harbour Principles, and to require that such data flows are only carried out under other instruments and provided they contain the necessary safeguards and guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals;
41. Calls on the Commission to present, by December 2014, a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities, and concrete recommendations based on the absence of a general data protection law in the US; encourages the Commission to engage with the US administration in order to establish a legal framework providing for a high level of protection of individuals with regard to the protection of their personal data when transferred to the US and ensure the equivalence of EU and US privacy frameworks;

*Transfers to other third countries with adequacy decision*

42. Recalls that Directive 95/46/EC stipulates that transfers of personal data to a third country may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection, the purpose of this provision being to ensure the continuity of the protection afforded by EU data protection law where personal data are transferred outside the EU;
43. Recalls that Directive 95/46/EC also provides that the adequacy of the level of protection afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation or set of such operations; recalls likewise that the said Directive also equips the Commission with implementing powers to declare that a third country ensures an adequate level of protection in the light of the criteria laid down by Directive 95/46/EC; recalls that Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;
44. Recalls that in the latter case Member States must take the measures necessary to prevent any transfer of data of the same type to the third country in question, and that the Commission should enter into negotiations with a view to remedying the situation;
45. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand Privacy Act and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by

Commission Decisions 2013/65 and 2/2002 of 20 December 2001, has been affected by the involvement of those countries' national intelligence agencies in the mass surveillance of EU citizens, and, if necessary, to take appropriate measures to suspend or reverse the adequacy decisions; also calls on the Commission to assess the situation for other countries that have received an adequacy rating; expects the Commission to report to Parliament on its findings on the above-mentioned countries by December 2014 at the latest;

*Transfers based on contractual clauses and other instruments*

46. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were formulated with situations of access to personal data for mass surveillance purposes in mind, and that such access would not be in line with the derogation clauses of the contractual clauses or BCRs which refer to exceptional derogations for a legitimate interest in a democratic society and where necessary and proportionate;
47. Calls on the Member States to prohibit or suspend data flows to third countries based on the standard contractual clauses, contractual clauses or BCRs authorised by the national competent authorities where it is likely that the law to which data recipients are subject imposes requirements on them which go beyond the restrictions that are strictly necessary, adequate and proportionate in a democratic society and are likely to have an adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create a risk of grave harm to the data subjects;
48. Calls on the Article 29 Working Party to issue guidelines and recommendations on the safeguards and protections that contractual instruments for international transfers of EU personal data should contain in order to ensure the protection of the privacy, fundamental rights and freedoms of individuals, taking particular account of the third-country laws on intelligence and national security and the involvement of the companies receiving the data in a third country in mass surveillance activities by a third country's intelligence agencies;
49. Calls on the Commission to examine without delay the standard contractual clauses it has established in order to assess whether they provide the necessary protection as regards access to personal data transferred under the clauses for intelligence purposes and, if appropriate, to review them;

*Transfers based on the Mutual Legal Assistance Agreement*

50. Calls on the Commission to conduct, before the end of 2014, an in-depth assessment of the existing Mutual Legal Assistance Agreement, pursuant to its Article 17, in order to verify its practical implementation and, in particular, whether the US has made effective use of it for obtaining information or evidence in the EU and whether the Agreement has been circumvented to acquire the information directly in the EU, and to assess the impact on the fundamental rights of individuals; such an assessment should not only refer to US official statements as a sufficient basis for the analysis but also be based on specific EU evaluations; this in-depth review should also address the

consequences of the application of the Union's constitutional architecture to this instrument in order to bring it into line with Union law, taking account in particular of Protocol 36 and Article 10 thereof and Declaration 50 concerning this protocol; calls on the Council and Commission also to assess bilateral agreements between Member States and the US so as to ensure that they are consistent with the agreements that the EU follows or decides to follow with the US;

*EU mutual assistance in criminal matters*

51. Asks the Council and Commission to inform Parliament about the actual use by Member States of the Convention on Mutual Assistance in Criminal Matters between the Member States, in particular its Title III on interception of telecommunications; calls on the Commission to put forward a proposal, in accordance with Declaration 50, concerning Protocol 36, as requested, before the end of 2014 in order to adapt it to the Lisbon Treaty framework;

*Transfers based on the TFTP and PNR agreements*

52. Takes the view that the information provided by the European Commission and the US Treasury does not clarify whether US intelligence agencies have access to SWIFT financial messages in the EU by intercepting SWIFT networks or banks' operating systems or communication networks, alone or in cooperation with EU national intelligence agencies and without having recourse to existing bilateral channels for mutual legal assistance and judicial cooperation;
53. Reiterates its resolution of 23 October 2013 and asks the Commission for the suspension of the TFTP Agreement;
54. Calls on the Commission to react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;

*Framework agreement on data protection in the field of police and judicial cooperation ('Umbrella Agreement')*

55. Considers that a satisfactory solution under the 'Umbrella agreement' is a precondition for the full restoration of trust between the transatlantic partners;
56. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should put rights for EU citizens on an equal footing with rights for US citizens; stresses that, moreover, this agreement should provide effective and enforceable administrative and judicial remedies for all EU citizens in the US without any discrimination;
57. Asks the Commission and Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes with the US as long as the 'Umbrella Agreement' has not entered into force;

58. Urges the Commission to report in detail on the various points of the negotiating mandate and the latest state of play by April 2014;

*Data protection reform*

59. Calls on the Council Presidency and the Member States to accelerate their work on the whole Data Protection Package to allow for its adoption in 2014, so that EU citizens will be able to enjoy a high level of data protection in the very near future; stresses that strong engagement and full support on the part of the Council are a necessary condition to demonstrate credibility and assertiveness towards third countries;
60. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals, and that the two must therefore be treated as a package to be adopted simultaneously, in order to ensure that all data-processing activities in the EU provide a high level of protection in all circumstances; stresses that it will only adopt further law enforcement cooperation measures once the Council has entered into negotiations with Parliament and the Commission on the Data Protection Package;
61. Recalls that the concepts of 'privacy by design' and 'privacy by default' are a strengthening of data protection and should have the status of guidelines for all products, services and systems offered on the internet;
62. Considers higher transparency and safety standards for online and telecommunication as a necessary principle with a view to a better data protection regime; calls, therefore, on the Commission to put forward a legislative proposal on standardised general terms and conditions for online and telecommunications services, and to mandate a supervisory body to monitor compliance with the general terms and conditions;

*Cloud computing*

63. Notes that trust in US cloud computing and cloud providers has been negatively affected by the above-mentioned practices; emphasises, therefore, the development of European clouds and IT solutions as an essential element for growth and employment and for trust in cloud computing services and providers, as well as for ensuring a high level of personal data protection;
64. Calls on all public bodies in the Union not to use cloud services where non-EU laws might apply;
65. Reiterates its serious concern regarding the compulsory direct disclosure of EU personal data and information processed under cloud agreements to third-country authorities by cloud providers subject to third-country laws or using storage servers located in third countries, as also regarding direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;
66. Deplores the fact that such access is usually attained by means of direct enforcement by third-country authorities of their own legal rules, without recourse to international

instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

67. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership while fully including civil society and the technical community, such as the Internet Engineering Task Force (IETF), and incorporating data protection aspects;
68. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges the Commission, furthermore, to take note of the negotiating partner's domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing services, in particular by demanding that such access be granted only if there is full respect for due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;
69. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches, and underlines the importance of having effective, proportionate and dissuasive administrative sanctions in place that can be imposed on 'cloud computing' service providers who do not comply with EU data protection standards;
70. Calls on the Commission and the competent authorities of the Member States to evaluate the extent to which EU rules on privacy and data protection have been violated through the cooperation of EU legal entities with secret services or through the acceptance of court warrants of third-country authorities requesting personal data of EU citizens contrary to EU data protection legislation;
71. Calls on businesses providing new services using 'Big Data' and new applications such as the 'Internet of Things' to build in data protection measures already at the development stage, in order to maintain a high level of trust among citizens;

*Transatlantic Trade and Investment Partnership Agreement (TTIP)*

72. Recognises that 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;
73. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the consent of the European Parliament to the final TTIP agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not completely abandoned and an adequate solution

is found for the data privacy rights of EU citizens, including administrative and judicial redress; stresses that Parliament may only consent to the final TTIP agreement provided the agreement fully respects, inter alia, the fundamental rights recognised by the EU Charter, and provided the protection of the privacy of individuals in relation to the processing and dissemination of personal data remain governed by Article XIV of the GATS; stresses that EU data protection legislation cannot be deemed an ‘arbitrary or unjustifiable discrimination’ in the application of Article XIV of the GATS;

### ***Democratic oversight of intelligence services***

74. Stresses that, despite the fact that oversight of intelligence services’ activities should be based on both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;
75. Calls, as it did in the case of Echelon, on all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on the national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means, including the right to conduct on-site visits, to be able to effectively control intelligence services;
76. Calls for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension;
77. Considers this High-Level group should:
  - define minimum European standards or guidelines on the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe), including the issue of oversight bodies being considered as a third party under the ‘third party rule’, or the principle of ‘originator control’, on the oversight and accountability of intelligence from foreign countries;
  - set strict limits on the duration and scope of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority; recalls that the duration of any surveillance ordered should be proportionate and limited to its purpose;
  - develop criteria on enhanced transparency, built on the general principle of access to information and the so-called ‘Tshwane Principles’<sup>1</sup>;
78. Intends to organise a conference with national oversight bodies, whether parliamentary or independent, by the end of 2014;

---

<sup>1</sup> The Global Principles on National Security and the Right to Information, June 2013.



79. Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;
80. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);
81. Urges the Commission and the HR/VP to present, by December 2014, a proposal for a legal basis for the activities of the EU Intelligence Analysis Centre (IntCen), together with an adequate oversight mechanism; urges the HR/VP to regularly account for the activities of IntCen to the responsible bodies of Parliament, including its full compliance with fundamental rights and applicable EU data privacy rules, and to specifically clarify its existing oversight mechanism with Parliament;
82. Calls on the Commission to present, by December 2014, a proposal for an EU security clearance procedure for all EU office holders, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;
83. Recalls the provisions of the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, which should be used to improve oversight at EU level;

### *EU agencies*

84. Calls on the Europol Joint Supervisory Body, together with national data protection authorities, to conduct a joint inspection before the end of 2014 in order to ascertain whether information and personal data shared with Europol have been lawfully acquired by national authorities, particularly if the information or data were initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data; considers that Europol should not process any information or data which were obtained in violation of fundamental rights which would be protected under the Charter of Fundamental Rights;
85. Calls on Europol to make full use of its mandate to request the competent authorities of the Member States to initiate criminal investigations with regards to major cyberattacks and IT breaches with potential cross-border impact; believes that Europol's mandate should be enhanced in order to allow it to initiate its own investigation following suspicion of a malicious attack on the network and information

systems of two or more Member States or Union bodies<sup>1</sup>; calls on the Commission to review the activities of Europol's European Cybercrime Centre (EC3) and, if necessary, put forward a proposal for a comprehensive framework for strengthening its competences;

### ***Freedom of expression***

86. Expresses its deep concern at the mounting threats to the freedom of the press and the chilling effect on journalists of intimidation by state authorities, in particular as regards the protection of confidentiality of journalistic sources; reiterates the calls expressed in its resolution of 21 May 2013 on ‘the EU Charter: standard settings for media freedom across the EU’;
87. Takes note of the detention of David Miranda and the seizure of the material in his possession by the UK authorities under Schedule 7 of the Terrorism Act 2000 (and also the request made to the *Guardian* newspaper to destroy or hand over the material) and expresses its concern that this constitutes a possible serious interference with the right of freedom of expression and media freedom as recognised by Article 10 of the ECHR and Article 11 of the EU Charter and that legislation intended to fight terrorism could be misused in such instances;
88. Draws attention to the plight of whistleblowers and their supporters, including journalists following their revelations; calls on the Commission to conduct an examination as to whether a future legislative proposal establishing an effective and comprehensive European whistleblower protection programme, as already requested in Parliament’s resolution of 23 October 2013, should also include other fields of Union competence, with particular attention to the complexity of whistleblowing in the field of intelligence; calls on the Member States to thoroughly examine the possibility of granting whistleblowers international protection from prosecution;
89. Calls on the Member States to ensure that their legislation, notably in the field of national security, provides a safe alternative to silence for disclosing or reporting of wrongdoing, including corruption, criminal offences, breaches of legal obligation, miscarriages of justice and abuse of authority, which is also in line with the provisions of different international (UN and Council of Europe) instruments against corruption, the principles laid out in the PACE Resolution 1729 (2010), the Tshwane principles, etc;

### ***EU IT security***

90. Points out that recent incidents clearly demonstrate the acute vulnerability of the EU, and in particular the EU institutions, national governments and parliaments, major European companies, European IT infrastructures and networks, to sophisticated attacks using complex software and malware; notes that these attacks require financial

---

<sup>1</sup> European Parliament legislative resolution of ... February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) (A7-0096/2014).

and human resources on a scale such that they are likely to originate from state entities acting on behalf of foreign governments; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack on the EU's IT capacity; underlines that boosting EU IT capacity and security also reduces the vulnerability of the EU towards serious cyberattacks originating from large criminal organisations or terrorist groups;

91. Takes the view that the mass surveillance revelations that have initiated this crisis can be used as an opportunity for Europe to take the initiative and build up, as a strategic priority measure, a strong and autonomous IT key-resource capability; stresses that in order to regain trust, such a European IT capability should be based, as much as possible, on open standards and open-source software and if possible hardware, making the whole supply chain from processor design to application layer transparent and reviewable; points out that in order to regain competitiveness in the strategic sector of IT services, a 'digital new deal' is needed, with joint and large-scale efforts by EU institutions, Member States, research institutions, industry and civil society; calls on the Commission and the Member States to use public procurement as leverage to support such resource capability in the EU by making EU security and privacy standards a key requirement in the public procurement of IT goods and services; urges the Commission, therefore, to review the current public procurement practices with regard to data processing in order to consider restricting tender procedures to certified companies, and possibly to EU companies, where security or other vital interests are involved;
92. Strongly condemns the fact that intelligence services sought to lower IT security standards and to install backdoors in a wide range of IT systems; asks the Commission to present draft legislation to ban the use of backdoors by law enforcement agencies; recommends, consequently, the use of open-source software in all environments where IT security is a concern;
93. Calls on all the Member States, the Commission, the Council and the European Council to give their fullest support, including through funding in the field of research and development, to the development of European innovative and technological capability in IT tools, companies and providers (hardware, software, services and network), including for purposes of cybersecurity and encryption and cryptographic capabilities;
94. Calls on the Commission, standardisation bodies and ENISA to develop, by December 2014, minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data and the integrity of all IT systems; believes that such standards could become the benchmark for new global standards and should be set in an open and democratic process, rather than being driven by a single country, entity or multinational company; takes the view that, while legitimate law enforcement and intelligence concerns need to be taken into account in order to support the fight against terrorism, they should not lead to a general undermining of the dependability of all IT systems; expresses support for the recent decisions by the Internet Engineering Task Force (IETF) to include governments in the threat model for internet security;

95. Points out that EU and national telecom regulators, and in certain cases also telecom companies, have clearly neglected the IT security of their users and clients; calls on the Commission to make full use of its existing powers under the ePrivacy and Telecommunication Framework Directive to strengthen the protection of confidentiality of communication by adopting measures to ensure that terminal equipment is compatible with the right of users to control and protect their personal data, and to ensure a high level of security of telecommunication networks and services, including by way of requiring state-of-the-art end-to-end encryption of communications;
96. Supports the EU cyber strategy, but considers that it does not cover all possible threats and should be extended to cover malicious state behaviour; underlines the need for more robust IT security and resilience of IT systems;
97. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop greater EU independence in the IT sector, including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, encryption and anonymisation) and to the protection of critical IT infrastructure (including in terms of ownership and vulnerability);
98. Calls on the Commission, in the framework of the next Work Programme of the Horizon 2020 Programme, to direct more resources towards boosting European research, development, innovation and training in the field of IT, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, the best possible security solutions including open-source security, and other information society services, and also to promote the internal market in European software, hardware, and encrypted means of communication and communication infrastructures, including by developing a comprehensive EU industrial strategy for the IT industry; considers that small and medium enterprises play a particular role in research; stresses that no EU funding should be granted to projects having the sole purpose of developing tools for gaining illegal access into IT systems;
99. Asks the Commission to map out current responsibilities and to review, by December 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for ENISA, Europol's Cyber Crime Centre and other Union centres of specialised expertise, CERT-EU and the EDPS, in order to enable them to play a key role in securing European communication systems, be more effective in preventing and investigating major IT breaches in the EU and performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches; in particular, calls on the Commission to consider strengthening ENISA's role in defending the internal systems within the EU institutions and to establish within ENISA's structure a Computer Emergency Response Team (CERT) for the EU and its Member States;
100. Requests the Commission to assess the need for an EU IT Academy that brings together the best independent European and international experts in all related fields, tasked with providing all relevant EU institutions and bodies with scientific advice on IT technologies, including security-related strategies;

101. Calls on the competent services of the Secretariat of the European Parliament, under the responsibility of the President of Parliament, to carry out, by December 2014 at the latest, a thorough review and assessment of Parliament's IT security dependability, focused on: budgetary means, staff resources, technical capabilities, internal organisation and all relevant elements, in order to achieve a high level of security for Parliament's IT systems; believes that such an assessment should at the least provide information, analysis and recommendations on:

- the need for regular, rigorous and independent security audits and penetration tests, with the selection of outside security experts ensuring transparency and guarantees of their credentials vis-à-vis third countries or any types of vested interest;
- the inclusion in tender procedures for new IT systems of best-practice specific IT security/privacy requirements, including the possibility of a requirement for open-source software as a condition of purchase or a requirement that trusted European companies should take part in the tender when sensitive, security-related areas are concerned;
- the list of companies under contract with Parliament in the IT and telecom fields, taking into account any information that has come to light about their cooperation with intelligence agencies (such as revelations about NSA contracts with a company such as RSA, whose products Parliament is using to supposedly protect remote access to their data by its Members and staff), including the feasibility of providing the same services by other, preferably European, companies;
- the reliability and resilience of the software, and especially off-the-shelf commercial software, used by the EU institutions in their IT systems with regard to penetrations and intrusions by EU or third-country law enforcement and intelligence authorities, taking also into account relevant international standards, best-practice security risk management principles, and adherence to EU Network Information Security standards on security breaches;
- the use of more open-source systems;
- steps and measures to take in order to address the increased use of mobile tools (e.g. smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;
- the security of the communications between the different workplaces of the Parliament and of the IT systems used in Parliament;
- the use and location of servers and IT centres for Parliament's IT systems and the implications for the security and integrity of the systems;
- the implementation in reality of the existing rules on security breaches and prompt notification of the competent authorities by the providers of publicly

available telecommunication networks;

- the use of cloud computing and storage services by Parliament, including the nature of the data stored in the cloud, how the content and access to it is protected and where the cloud-servers are located, clarifying the applicable data protection and intelligence legal framework, as well as assessing the possibilities of solely using cloud servers that are based on EU territory;
  - a plan allowing for the use of more cryptographic technologies, in particular end-to-end authenticated encryption for all IT and communications services such as cloud computing, email, instant messaging and telephony;
  - the use of electronic signatures in email;
  - a plan for using a default encryption standard, such as the GNU Privacy Guard, for emails that would at the same time allow for the use of digital signatures;
  - the possibility of setting up a secure instant messaging service within Parliament allowing secure communication, with the server only seeing encrypted content;
102. Calls for all the EU institutions and agencies to perform a similar exercise in cooperation with ENISA, Europol and the CERTs, by December 2014 at the latest, in particular the European Council, the Council, the European External Action Service (including EU delegations), the Commission, the Court of Justice and the European Central Bank; invites the Member States to conduct similar assessments;
103. Stresses that as far as the external action of the EU is concerned, assessments of related budgetary needs should be carried out and first measures taken without delay in the case of the European External Action Service (EEAS) and that appropriate funds need to be allocated in the 2015 draft budget;
104. Takes the view that the large-scale IT systems used in the area of freedom, security and justice, such as the Schengen Information System II, the Visa Information System, Eurodac and possible future systems such as EU-ESTA, should be developed and operated in such a way as to ensure that data are not compromised as a result of requests by authorities from third countries; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;
105. Calls on the Commission and the EEAS to take action at the international level, with the UN in particular, and in cooperation with interested partners to implement an EU strategy for democratic governance of the internet in order to prevent undue influence over ICANN's and IANA's activities by any individual entity, company or country by ensuring appropriate representation of all interested parties in these bodies, while avoiding the facilitation of state control or censorship or the balkanisation and fragmentation of the internet;
106. Calls for the EU to take the lead in reshaping the architecture and governance of the internet in order to address the risks related to data flows and storage, striving for

more data minimisation and transparency and less centralised mass storage of raw data, as well as for rerouting of Internet traffic or full end-to-end encryption of all Internet traffic so as to avoid the current risks associated with unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy ;

107. Calls for the promotion of
- EU search engines and EU social networks as a valuable step in the direction of IT independence for the EU;
  - European IT service providers;
  - encrypting communication in general, including email and SMS communication;
  - European IT key elements, for instance solutions for client-server operating systems, using open-source standards, developing European elements for grid coupling, e.g. routers;
108. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to develop a culture of security and to launch an education and awareness-raising campaign in order to enable citizens to make a more informed choice regarding what personal data to put on-line and how better to protect them, including through encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;
109. Calls on the Commission, by December 2014, to put forward legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data; in this respect, calls on the Commission to evaluate the possibility of setting up a certification or validation scheme for IT hardware including testing procedures at EU level to ensure the integrity and security of the products;

### ***Rebuilding trust***

110. Believes that, beyond the need for legislative change, the inquiry has shown the need for the US to restore trust with its EU partners, as it is the US intelligence agencies' activities that are primarily at stake;
111. Points out that the crisis of confidence generated extends to:
- the spirit of cooperation within the EU, as some national intelligence activities may jeopardise the attainment of the Union's objectives;

- citizens, who realise that not only third countries or multinational companies but also their own government may be spying on them;
- respect for fundamental rights, democracy and the rule of law, as well as the credibility of democratic, judicial and parliamentary safeguards and oversight in a digital society;

*Between the EU and the US*

112. Recalls the important historical and strategic partnership between the EU Member States and the US, based on a common belief in democracy, the rule of law and fundamental rights;
113. Believes that the mass surveillance of citizens and the spying on political leaders by the US have caused serious damage to relations between the EU and the US and negatively impacted on trust in US organisations acting in the EU; this is further exacerbated by the lack of judicial and administrative remedies for redress under US law for EU citizens, particularly in cases of surveillance activities for intelligence purposes;
114. Recognises, in light of the global challenges facing the EU and the US, that the transatlantic partnership needs to be further strengthened, and that it is vital that transatlantic cooperation in counter-terrorism continues on a new basis of trust based on true common respect for the rule of law and the rejection of all indiscriminate practices of mass surveillance; insists, therefore, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;
115. Is ready to engage in a dialogue with US counterparts so that, in the ongoing American public and congressional debate on reforming surveillance and reviewing intelligence oversight, the right to privacy and other rights of EU citizens, residents or other persons protected by EU law and equivalent information rights and privacy protection in US courts, including legal redress, are guaranteed through, for example, a revision of the Privacy Act and the Electronic Communications Privacy Act and by ratifying the First Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR), so that the current discrimination is not perpetuated;
116. Insists that necessary reforms be undertaken and effective guarantees be given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is proportional, limited by clearly specified conditions, and related to reasonable suspicion and probable cause of terrorist activity; stresses that this purpose must be subject to transparent judicial oversight;
117. Considers that clear political signals are needed from our American partners to demonstrate that the US distinguishes between allies and adversaries;
118. Urges the Commission and the US Administration to address, in the context of the ongoing negotiations on an EU-US Umbrella Agreement on data transfer for law enforcement purposes, the information and judicial redress rights of EU citizens, and



to conclude these negotiations, in line with the commitment made at the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, before summer 2014;

119. Encourages the US to accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis between the transatlantic allies;
120. Calls on the EU institutions to explore the possibilities for establishing with the US a code of conduct which would guarantee that no US espionage is pursued against EU institutions and facilities;

*Within the European Union*

121. Also believes that the involvement and activities of EU Member States have led to a loss of trust, including among Member States and between EU citizens and their national authorities; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including an end to mass surveillance activities and strengthening the system of judicial and parliamentary oversight, will it be possible to re-establish the trust lost; reiterates the difficulties involved in developing comprehensive EU security policies with such mass surveillance activities in operation, and stresses that the EU principle of sincere cooperation requires that Member States refrain from conducting intelligence activities in other Member States' territory;
122. Notes that some Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (the UK) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; stresses that these Member States need to observe fully the interests and the legislative framework of the EU as a whole; deems such bilateral arrangements to be counterproductive and irrelevant, given the need for a European approach to this problem; asks the Council to inform Parliament on developments by Member States on an EU-wide mutual no-spy arrangement;
123. Considers that such arrangements should not breach the Union Treaties, especially the principle of sincere cooperation (under Article 4(3) TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition, and economic, industrial and social development; decides to review any such arrangements for their compatibility with European law, and reserves the right to activate Treaty procedures in the event of such arrangements being proven to contradict the Union's cohesion or the fundamental principles on which it is based;
124. Calls on the Member States to make every effort to ensure better cooperation with a view to providing safeguards against espionage, in cooperation with the relevant EU bodies and agencies, for the protection of EU citizens and institutions, European companies, EU industry, and IT infrastructure and networks, as well as European research; considers the active involvement of EU stakeholders to be a precondition for an effective exchange of information; points out that security threats have become

more international, diffuse and complex, thereby requiring an enhanced European cooperation; believes that this development should be better reflected in the Treaties, and therefore calls for a revision of the Treaties in order to reinforce the notion of sincere cooperation between the Member States and the Union as regards the objective of achieving an area of security and to prevent mutual espionage between Member States within the Union;

125. Considers tap-proof communication structures (email and telecommunications, including landlines and cell phones) and tap-proof meeting rooms within all relevant EU institutions and EU delegations to be absolutely necessary; therefore calls for the establishment of an encrypted internal EU email system;
126. Calls on the Council and Commission to consent without further delay to the proposal adopted by the European Parliament on 23 May 2012 for a regulation of the European Parliament on the detailed provisions governing the exercise of the European Parliament's right of inquiry and repealing Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission presented on the basis of Article 226 TFEU; calls for a revision of the Treaty in order to extend such inquiry powers to cover, without restrictions or exceptions, all fields of Union competence or activity and to include the possibility of questioning under oath;

#### *Internationally*

127. Calls on the Commission to present, by January 2015 at the latest, an EU strategy for democratic governance of the internet;
128. Calls on the Member States to follow the call of the 35th International Conference of Data Protection and Privacy Commissioners 'to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in the Human Rights Committee General Comment No 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law'; calls on the Member States to include in this exercise a call for an international UN agency to be in charge of, in particular, monitoring the emergence of surveillance tools and regulating and investigating their uses; asks the High Representative/Vice-President of the Commission and the European External Action Service to take a proactive stance;
129. Calls on the Member States to develop a coherent and strong strategy within the UN, supporting in particular the resolution on 'the right to privacy in the digital age' initiated by Brazil and Germany, as adopted by the Third Committee of the UN General Assembly Committee (Human Rights Committee) on 27 November 2013, as well as taking further action for the defence of the fundamental right to privacy and data protection at an international level while avoiding any facilitation of state control or censorship or the fragmentation of the internet, including an initiative for an international treaty prohibiting mass surveillance activities and an agency for its oversight;

***Priority Plan: A European Digital Habeas Corpus - protecting fundamental rights in a digital age***

130. Decides to submit to EU citizens, institutions and Member States the above-mentioned recommendations as a Priority Plan for the next legislature;

131. Decides to launch ‘A European Digital Habeas Corpus - protecting fundamental rights in a digital age’ with the following 8 actions, the implementation of which it will oversee:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law enforcement purposes;

Action 3: Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with the highest EU standards;

Action 4: Suspend the TFTP agreement until: (i) the Umbrella Agreement negotiations have been concluded; (ii) a thorough investigation has been concluded on the basis of an EU analysis and all concerns raised by Parliament in its resolution of 23 October 2013 have been properly addressed;

Action 5: Evaluate any agreement, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data is not violated due to surveillance activities, and take necessary follow-up actions;

Action 6: Protect the rule of law and the fundamental rights of EU citizens, (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring enhanced protection for whistleblowers;

Action 7: Develop a European strategy for greater IT independence (a ‘digital new deal’ including the allocation of adequate resources at national and EU level) in order to boost IT industry and allow European companies to exploit the EU privacy competitive advantage;

Action 8: Develop the EU as a reference player for a democratic and neutral governance of the internet;

132. Calls on the EU institutions and the Member States to promote the ‘European Digital Habeas Corpus’ protecting fundamental rights in a digital age; undertakes to act as the EU citizens’ rights advocate, with the following timetable to monitor implementation:

- April-July 2014: a monitoring group based on the LIBE inquiry team responsible for monitoring any new revelations concerning the inquiry's mandate and scrutinising the implementation of this resolution;
  - July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;
  - Spring 2014: a formal call on the European Council to include the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' - in the guidelines to be adopted under Article 68 TFEU;
  - Autumn 2014: a commitment that the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' and related recommendations will serve as key criteria for the approval of the next Commission;
  - 2014: a conference bringing together high-level European experts in the various fields conducive to IT security (including mathematics, cryptography and privacy-enhancing technologies) to help foster an EU IT strategy for the next legislative term;
  - 2014-2015: a Trust/Data/Citizens' Rights group to be convened on a regular basis between the European Parliament and the US Congress, as well as with other committed third-country parliaments, including that of Brazil;
  - 2014-2015: a conference with the intelligence oversight bodies of European national parliaments;
133. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, the national data protection authorities, the EDPS, eu-LISA, ENISA, the Fundamental Rights Agency, the Article 29 Working Party, the Council of Europe, the Congress of the United States of America, the US Administration, the President, Government and Parliament of the Federative Republic of Brazil, and the UN Secretary-General.

## EXPLANATORY STATEMENT

*'The office of the sovereign, be it a monarch or an assembly, consisteth in the end,  
for which he was trusted with the sovereign power,  
namely the procuration of the safety of people'  
Hobbes, Leviathan (chapter XXX)*

*'We cannot commend our society to others by departing  
from the fundamental standards which  
make it worthy of commendation'  
Lord Bingham of Cornhill,  
Former Lord Chief Justice of England and Wales*

### **Methodology**

From July 2013, the LIBE Committee of Inquiry was responsible for the extremely challenging task of fulfilling the mandate<sup>1</sup> of the Plenary on the investigation into the electronic mass surveillance of EU citizens in a very short timeframe, less than 6 months.

During that period it held over 15 hearings covering each of the specific cluster issues prescribed in the 4 July resolution, drawing on the submissions of both EU and US experts representing a wide range of knowledge and backgrounds: EU institutions, national parliaments, US congress, academics, journalists, civil society, security and technology specialists and private business. In addition, a delegation of the LIBE Committee visited Washington on 28-30 October 2013 to meet with representatives of both the executive and the legislative branch (academics, lawyers, security experts, business representatives)<sup>2</sup>. A delegation of the Committee on Foreign Affairs (AFET) was also in town at the same time. A few meetings were held together.

A series of working documents<sup>3</sup> have been co-authored by the rapporteur, the shadow-rapporteurs<sup>4</sup> from the various political groups and 3 Members from the AFET Committee<sup>5</sup> enabling a presentation of the main findings of the Inquiry. The rapporteur would like to thank all shadow rapporteurs and AFET Members for their close cooperation and high-level commitment throughout this demanding process.

### **Scale of the problem**

**An increasing focus on security combined with developments in technology has enabled States to know more about citizens than ever before.** By being able to collect data

---

<sup>1</sup> [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/ta/04/07/2013%20-%200322/p7\\_ta-prov\(2013\)0322\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_en.pdf)

<sup>2</sup> See Washington delegation report.

<sup>3</sup> See Annex I.

<sup>4</sup> List of shadow rapporteurs: Axel Voss (EPP), Sophia in't Veld (ALDE), Jan Philipp Albrecht (GREENS/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).

<sup>5</sup> List of AFET Members: José Ignacio Salafranca Sánchez-Neyra (EPP), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).

regarding the content of communications, as well as metadata, and by following citizens' electronic activities, in particular their use of smartphones and tablet computers, intelligence services are de facto able to know almost everything about a person. This has **contributed to a fundamental shift in the work and practices of intelligence agencies, away from the traditional concept of targeted surveillance as a necessary and proportional counter-terrorism measure, towards systems of mass surveillance.**

**This process of increasing mass surveillance has not been subject to any prior public debate or democratic decision-making. Discussion is needed on the purpose and scale of surveillance and its place in a democratic society. Is the situation created by Edward Snowden's revelations an indication of a general societal turn towards the acceptance of the death of privacy in return for security?** Do we face a breach of privacy and intimacy so great that it is possible not only for criminals but for IT companies and intelligence agencies to know every detail of the life of a citizen? Is it a fact to be accepted without further discussion? Or is the responsibility of the legislator to adapt the policy and legal tools at hand to limit the risks and prevent further damages in case less democratic forces would come to power?

### **Reactions to mass surveillance and a public debate**

The debate on mass surveillance does not take place in an even manner inside the EU. In fact in many Member States there is hardly any public debate and media attention varies. Germany seems to be the country where reactions to the revelations have been strongest and public discussions as to their consequences have been widespread. In the United Kingdom and France, in spite of investigations by The Guardian and Le Monde, reactions seem more limited, a fact that has been linked to the alleged involvement of their national intelligence services in activities with the NSA. The LIBE Committee Inquiry has been in a position to hear valuable contributions from the parliamentary oversight bodies of Belgian, the Netherlands, Denmark and even Norway; however the British and French Parliament have declined participation. These differences show again the uneven degree of checks and balances within the EU on these issues and that more cooperation is needed between parliamentary bodies in charge of oversight.

Following the disclosures of Edward Snowden in the mass media, public debate has been based on two main types of reactions. On the one hand, there are those who deny the legitimacy of the information published on the grounds that most of the media reports are based on misinterpretation; in addition many argue, while not having refuted the disclosures, the validity of the disclosures made due to allegations of security risks they cause for national security and the fight against terrorism.

On the other hand, there are those who consider the information provided requires an informed, public debate because of the magnitude of the problems it raises to issues key to a democracy including: the rule of law, fundamental rights, citizens' privacy, public accountability of law-enforcement and intelligence services, etc. This is certainly the case for the journalists and editors of the world's biggest press outlets who are privy to the disclosures including The Guardian, Le Monde, Der Spiegel, The Washington Post and Glenn Greenwald.

The two types of reactions outlined above are based on a set of reasons which, if followed,

may lead to quite opposed decisions as to how the EU should or should not react.

### **5 reasons not to act**

– *The ‘Intelligence/national security argument’: no EU competence*

Edward Snowden’s revelations relate to US and some Member States’ intelligence activities, but national security is a national competence, the EU has no competence in such matters (except on EU internal security) and therefore no action is possible at EU level.

– *The ‘Terrorism argument’: danger of the whistleblower*

Any follow up to these revelations, or their mere consideration, further weakens the security of the US as well as the EU as it does not condemn the publication of documents the content of which even if redacted as involved media players explain may give valuable information to terrorist groups.

– *The ‘Treason argument: no legitimacy for the whistleblower*

As mainly put forward by some in the US and in the United Kingdom, any debate launched or action envisaged further to E. Snowden’s revelations is intrinsically biased and irrelevant as they would be based on an initial act of treason.

– *The ‘realism argument’: general strategic interests*

Even if some mistakes and illegal activities were to be confirmed, they should be balanced against the need to maintain the special relationship between the US and Europe to preserve shared economic, business and foreign policy interests.

– *The ‘Good government argument’: trust your government*

US and EU Governments are democratically elected. In the field of security, and even when intelligence activities are conducted in order to fight against terrorism, they comply with democratic standards as a matter of principle. This ‘presumption of good and lawful governance’ rests not only on the goodwill of the holders of the executive powers in these states but also on the checks and balances mechanism enshrined in their constitutional systems.

As one can see reasons not to act are numerous and powerful. This may explain why most EU governments, after some initial strong reactions, have preferred not to act. The main action by the Council of Ministers has been to set up a ‘transatlantic group of experts on data protection’ which has met 3 times and put forward a final report. A second group is supposed to have met on intelligence related issues between US authorities and Member States’ ones but no information is available. The European Council has addressed the surveillance problem in a mere statement of Heads of state or government<sup>1</sup>, Up until now only a few national

---

<sup>1</sup> European Council Conclusions of 24-25 October 2013, in particular: ‘The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before

parliaments have launched inquiries.

### **5 reasons to act**

- *The ‘mass surveillance argument’: in which society do we want to live?*

Since the very first disclosure in June 2013, consistent references have been made to George’s Orwell novel ‘1984’. Since 9/11 attacks, a focus on security and a shift towards targeted and specific surveillance has seriously damaged and undermined the concept of privacy. The history of both Europe and the US shows us the dangers of mass surveillance and the graduation towards societies without privacy.

- *The ‘fundamental rights argument’:*

*Mass and indiscriminate surveillance threaten citizens’ fundamental rights including right to privacy, data protection, freedom of press, fair trial which are all enshrined in the EU Treaties, the Charter of fundamental rights and the ECHR. These rights cannot be circumvented nor be negotiated against any benefit expected in exchange unless duly provided for in legal instruments and in full compliance with the treaties.*

- *The ‘EU internal security argument’:*

National competence on intelligence and national security matters does not exclude a parallel EU competence. The EU has exercised the competences conferred upon it by the EU Treaties in matters of internal security by deciding on a number of legislative instruments and international agreements aimed at fighting serious crime and terrorism, on setting-up an internal security strategy and agencies working in this field. In addition, other services have been developed reflecting the need for increased cooperation at EU level on intelligence-related matters: INTCEN (placed within EEAS) and the Anti-terrorism Coordinator (placed within the Council general secretariat), neither of them with a legal basis.

- *The ‘deficient oversight argument’*

*While intelligence services perform an indispensable function in protecting against internal and external threats, they have to operate within the rule of law and to do so must be subject to a stringent and thorough oversight mechanism. The democratic oversight of intelligence activities is conducted at national level but due to the international nature of security threats there is now a huge exchange of information between Member States and with third countries like the US; improvements in oversight mechanisms are needed both at national and at EU level if traditional oversight mechanisms are not to become ineffective and outdated.*

- *The ‘chilling effect on media’ and the protection of whistleblowers*

The disclosures of Edward Snowden and the subsequent media reports have highlighted the

---

the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative. They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect’.



pivotal role of the media in a democracy to ensure accountability of Governments. When supervisory mechanisms fail to prevent or rectify mass surveillance, the role of media and whistleblowers in unveiling eventual illegalities or misuses of power is extremely important. Reactions from the US and UK authorities to the media have shown the vulnerability of both the press and whistleblowers and the urgent need to do more to protect them.

The European Union is called on to choose between a ‘business as usual’ policy (sufficient reasons not to act, wait and see) and a ‘reality check’ policy (surveillance is not new, but there is enough evidence of an unprecedented magnitude of the scope and capacities of intelligence agencies requiring the EU to act).

### **Habeas Corpus in a Surveillance Society**

In 1679 the British parliament adopted the Habeas Corpus Act as a major step forward in securing the right to a judge in times of rival jurisdictions and conflicts of laws. Nowadays our democracies ensure proper rights for a convicted or detainee who is in person physically subject to a criminal proceeding or deferred to a court. But his or her data, as posted, processed, stored and tracked on digital networks form a ‘body of personal data’, a kind of digital body specific to every individual and enabling to reveal much of his or her identity, habits and preferences of all types.

Habeas Corpus is recognised as a fundamental legal instrument to safeguarding individual freedom against arbitrary state action. What is needed today is an extension of Habeas Corpus to the digital era. Right to privacy, respect of the integrity and the dignity of the individual are at stake. Mass collections of data with no respect for EU data protection rules and specific violations of the proportionality principle in the data management run counter to the constitutional traditions of the Member States and the fundamentals of the European constitutional order.

The main novelty today is these risks do not only originate in criminal activities (against which the EU legislator has adopted a series of instruments) or from possible cyber-attacks from governments of countries with a lower democratic record. There is a realisation that such risks may also come from law-enforcement and intelligence services of democratic countries putting EU citizens or companies under conflicts of laws resulting in a lesser legal certainty, with possible violations of rights without proper redress mechanisms.

Governance of networks is needed to ensure the safety of personal data. Before modern states developed, no safety on roads or city streets could be guaranteed and physical integrity was at risk. Nowadays, despite dominating everyday life, information highways are not secure. Integrity of digital data must be secured, against criminals of course but also against possible abuse of power by state authorities or contractors and private companies under secret judicial warrants.

### **LIBE Committee Inquiry Recommendations**

Many of the problems raised today are extremely similar to those revealed by the European Parliament Inquiry on the Echelon programme in 2001. The impossibility for the previous legislature to follow up on the findings and recommendations of the Echelon Inquiry should serve as a key lesson to this Inquiry. It is for this reason that this Resolution, recognising both

the magnitude of the revelations involved and their ongoing nature, is forward planning and ensures that there are specific proposals on the table for follow up action in the next Parliamentary mandate ensuring the findings remain high on the EU political agenda.

Based on this assessment, the rapporteur would like to submit to the vote of the Parliament the following measures:

**‘A European Digital Habeas corpus - protecting fundamental rights in a digital age’ based on 8 actions:**

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law-enforcement purposes;

Action 3: Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with highest EU standards;

Action 4: Suspend the TFTP agreement until (i) the Umbrella Agreement negotiations have been concluded; (ii) a thorough investigation has been concluded on the basis of an EU analysis, and all concerns raised by Parliament in its resolution of 23 October 2013 have been properly addressed;

Action 5: Evaluate any agreement, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data are not violated due to surveillance activities and take necessary follow-up actions;

Action 6: Protect the rule of law and the fundamental rights of EU citizens, (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 7: Develop a European strategy for greater IT independence (a ‘digital new deal’ including the allocation of adequate resources at national and EU level) to boost IT industry and allow European companies to exploit the EU privacy competitive advantage;

Action 8: Develop the EU as a reference player for a democratic and neutral governance of the internet;

After the conclusion of the Inquiry the European Parliament should continue acting as EU citizens’ rights advocate with the following timetable to monitor implementations:

- April-July 2014: a monitoring group based on the LIBE inquiry team

responsible for monitoring any new revelations concerning the inquiry's mandate and scrutinising the implementation of this resolution;

- July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;
- Spring 2014: a formal call on the European Council to include the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' - in the guidelines to be adopted under Article 68 TFEU;
- Autumn 2014: a commitment that the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' and related recommendations will serve as key criteria for the approval of the next Commission;
- 2014: a conference bringing together high-level European experts in the various fields conducive to IT security (including mathematics, cryptography and privacy-enhancing technologies) to help foster an EU IT strategy for the next legislature;
- 2014-2015: a Trust/Data/Citizens' Rights group to be convened on a regular basis between the European Parliament and the US Congress, as well as with other committed third-country parliaments, including Brazil;
- 2014-2015: a conference with the intelligence oversight bodies of European national parliaments;

## ANNEX I: LIST OF WORKING DOCUMENTS

### LIBE Committee Inquiry

<b>Rapporteur &amp; Shadows as co-authors</b>	<b>Issues</b>	<b>EP resolution of 4 July 2013 (see paragraphs 15-16)</b>
Mr Moraes (S&D)	US and EU Member Surveillance programmes and their impact on EU citizens fundamental rights	16 (a) (b) (c) (d)
Mr Voss (EPP)	US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation	16 (a) (b) (c)
Mrs In't Veld (ALDE) & Mrs Ernst (GUE)	Democratic oversight of Member State intelligence services and of EU intelligence bodies.	15, 16 (a) (c) (e)
Mr Albrecht (GREENS/EF A)	The relation between the surveillance practices in the EU and the US and the EU data protection provisions	16 (c) (e) (f)
Mr Kirkhope (ECR)	Scope of International, European and national security in the EU perspective <sup>1</sup>	16 (a) (b)
AFET 3 Members	Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens	16 (a) (b) (f)

---

<sup>1</sup> Not delivered.

## ANNEX II: LIST OF HEARINGS AND EXPERTS

### LIBE COMMITTEE INQUIRY ON US NSA SURVEILLANCE PROGRAMME, SURVEILLANCE BODIES IN VARIOUS MEMBER STATES AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS AND ON TRANSATLANTIC COOPERATION IN JUSTICE AND HOME AFFAIRS

Following the European Parliament resolution of 4th July 2013 (para. 16), the LIBE Committee has held a series of hearings to gather information relating the different aspects at stake, assess the impact of the surveillance activities covered, notably on fundamental rights and data protection rules, explore redress mechanisms and put forward recommendations to protect EU citizens' rights, as well as to strengthen IT security of EU Institutions.

Date	Subject	Experts
5 <sup>th</sup> September 2013 15.00 – 18.30 (BXL)	<ul style="list-style-type: none"> <li>- Exchange of views with the journalists unveiling the case and having made public the facts</li>   <li>- Follow-up of the Temporary Committee on the ECHELON Interception System</li> </ul>	<ul style="list-style-type: none"> <li>• Jacques FOLLOROU, Le Monde</li> <li>• Jacob APPELBAUM, investigative journalist, software developer and computer security researcher with the Tor Project</li> <li>• Alan RUSBRIDGER, Editor-in-Chief of Guardian News and Media (via videoconference)</li>   <li>• Carlos COELHO (MEP), former Chair of the Temporary Committee on the ECHELON Interception System</li> <li>• Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001)</li> <li>• Duncan CAMPBELL, investigative journalist and author of the STOA report 'Interception Capabilities 2000'</li> </ul>
12 <sup>th</sup> September 2013 10.00 – 12.00	- Feedback of the meeting of the EU-US Transatlantic group of experts on data protection of 19/20	<ul style="list-style-type: none"> <li>• Darius ŽILYS, Council Presidency, Director International Law Department,</li> </ul>

(STR)	<p>September 2013 - working method and cooperation with the LIBE Committee Inquiry (In camera)</p> <p>- Exchange of views with Article 29 Data Protection Working Party</p>	<p>Lithuanian Ministry of Justice (co-chair of the EU-US ad hoc working group on data protection)</p> <ul style="list-style-type: none"> <li>• Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection)</li> <li>• Reinhard PRIEBE, Director DG HOME, European Commission (co-chair of the EU-US ad hoc working group on data protection)</li> <li>• Jacob KOHNSTAMM, Chairman</li> </ul>
<p>24<sup>th</sup> September 2013 9.00 – 11.30 and 15.00 - 18h30 (BXL)</p> <p><b>With AFET</b></p>	<p>- Allegations of NSA tapping into the SWIFT data used in the TFTP programme</p> <p>- Feedback of the meeting of the EU-US Transatlantic group of experts on data protection of 19/20 September 2013</p> <p>- Exchange of views with US Civil Society (part I)</p>	<ul style="list-style-type: none"> <li>• Cecilia MALMSTRÖM, Member of the European Commission</li> <li>• Rob WAINWRIGHT, Director of Europol</li> <li>• Blanche PETRE, General Counsel of SWIFT</li> <li>• Darius ŽILYS, Council Presidency, Director International Law Department, Lithuanian Ministry of Justice (co-chair of the EU-US ad hoc working group on data protection)</li> <li>• Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection)</li> <li>• Reinhard PRIEBE, Director DG HOME, European Commission (co-chair of the EU-US ad hoc working group on data protection)</li> <li>• Jens-Henrik JEPPESEN, Director, European Affairs, Center for Democracy &amp; Technology (CDT)</li> <li>• Greg NOJEIM, Senior Counsel</li> </ul>

	<p>- Effectiveness of surveillance in fighting crime and terrorism in Europe</p> <p>- Presentation of the study on the US surveillance programmes and their impact on EU citizens' privacy</p>	<p>and Director of Project on Freedom, Security &amp; Technology, Center for Democracy &amp; Technology (CDT) (via videoconference)</p> <ul style="list-style-type: none"> <li>• Dr Reinhard KREISSL, Coordinator, Increasing Resilience in Surveillance Societies (IRISS) (via videoconference)</li> <li>• Caspar BOWDEN, Independent researcher, ex-Chief Privacy Adviser of Microsoft, author of the Policy Department note commissioned by the LIBE Committee on the US surveillance programmes and their impact on EU citizens' privacy</li> </ul>
<p>30th September 2013 15.00 - 18.30 (Bxl) <b>With AFET</b></p>	<p>- Exchange of views with US Civil Society (Part II)</p> <p>- Whistleblowers' activities in the field of surveillance and their legal protection</p>	<ul style="list-style-type: none"> <li>• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC)</li> <li>• Catherine CRUMP, American Civil Liberties Union (ACLU)</li> </ul> <p>Statements by whistleblowers:</p> <ul style="list-style-type: none"> <li>• Thomas DRAKE, ex-NSA Senior Executive</li> <li>• J. Kirk WIEBE, ex-NSA Senior analyst</li> <li>• Annie MACHON, ex-MI5 Intelligence officer</li> </ul> <p>Statements by NGOs on legal protection of whistleblowers:</p> <ul style="list-style-type: none"> <li>• Jesselyn RADACK, lawyer and representative of 6 whistleblowers, Government Accountability Project</li> <li>• John DEVITT, Transparency International Ireland</li> </ul>
<p>3<sup>rd</sup> October 2013 16.00 to 18.30 (BXL)</p>	<p>- Allegations of 'hacking' / tapping into the Belgacom systems by intelligence services (UK GCHQ)</p>	<ul style="list-style-type: none"> <li>• Mr Geert STANDAERT, Vice President Service Delivery Engine, BELGACOM S.A.</li> <li>• Mr Dirk LYBAERT, Secretary</li> </ul>

		<p>General, BELGACOM S.A.</p> <ul style="list-style-type: none"> <li>• Mr Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, co-rapporteur ‘dossier Belgacom’</li> </ul>
<p>7<sup>th</sup> October 2013 19.00 – 21.30 (STR)</p>	<p>- Impact of us surveillance programmes on the us safe harbour</p> <p>- impact of us surveillance programmes on other instruments for international transfers (contractual clauses, binding corporate rules)</p>	<ul style="list-style-type: none"> <li>• Dr Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (GERMANY)</li> <li>• Christopher CONNOLLY – Galexia</li> <li>• Peter HUSTINX, European Data Protection Supervisor (EDPS)</li> <li>• Ms Isabelle FALQUE-PIERROTIN, President of CNIL (FRANCE)</li> </ul>
<p>14<sup>th</sup> October 2013 15.00 - 18.30 (BXL)</p>	<p>- Electronic Mass Surveillance of EU Citizens and International,</p> <p>Council of Europe and</p> <p>EU Law</p> <p>- Court cases on Surveillance Programmes</p>	<ul style="list-style-type: none"> <li>• Martin SCHEININ, Former UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, Professor European University Institute and leader of the FP7 project ‘SURVEILLE’</li> <li>• Judge Bostjan ZUPANČIČ, Judge at the ECHR (via videoconference)</li> <li>• Douwe KORFF, Professor of Law, London Metropolitan University</li> <li>• Dominique GUIBERT, Vice-Président of the ‘Ligue des Droits de l’Homme’ (LDH)</li> <li>• Nick PICKLES, Director of Big Brother Watch</li> <li>• Constanze KURZ, Computer Scientist, Project Leader at Forschungszentrum für Kultur und Informatik</li> </ul>



<p>7<sup>th</sup> November 2013 9.00 – 11.30 and 15.00 - 18h30 (BXL)</p>	<p>- The role of EU IntCen in EU Intelligence activity (in Camera)</p> <p>- National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law</p> <p>- The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part I)<sup>54</sup> (Venice Commission) (UK)</p> <p>- EU-US transatlantic experts group</p>	<ul style="list-style-type: none"> <li>• Mr Ilkka SALMI, Director of EU Intelligence Analysis Centre (IntCen)</li> <li>• Dr Sergio CARRERA, Senior Research Fellow and Head of the JHA Section, Centre for European Policy Studies (CEPS), Brussels</li> <li>• Dr Francesco RAGAZZI, Assistant Professor in International Relations, Leiden University</li> <li>• Mr Iain CAMERON, Member of the European Commission for Democracy through Law - ‘Venice Commission’</li> <li>• Mr Ian LEIGH, Professor of Law, Durham University</li> <li>• Mr David BICKFORD, Former Legal Director of the Security and intelligence agencies MI5 and MI6</li> <li>• Mr Gus HOSEIN, Executive Director, Privacy International</li> <li>• Mr Paul NEMITZ, Director - Fundamental Rights and Citizenship, DG JUST, European Commission</li> <li>• Mr Reinhard PRIEBE, Director - Crisis Management and Internal Security, DG Home, European Commission</li> </ul>
<p>11<sup>th</sup> November 2013 15h-18.30 (BXL)</p>	<p>- US surveillance programmes and their impact on EU citizens’ privacy (statement by Mr Jim SENSENBRENNER, Member of the US Congress)</p> <p>- The role of Parliamentary oversight of intelligence services at</p>	<ul style="list-style-type: none"> <li>• Mr Jim SENSENBRENNER, US House of Representatives, (Member of the Committee on the Judiciary and Chairman of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations)</li> <li>• Mr Peter ERIKSSON, Chair of the Committee on the</li> </ul>

<sup>54</sup> Intelligence oversight bodies of the various EU National Parliaments have been invited to testify at the Inquiry

	<p>national level in an era of mass surveillance (NL,SW))(Part II)</p> <p>- US NSA programmes for electronic mass surveillance and the role of IT Companies (Microsoft, Google, Facebook)</p>	<p>Constitution, Swedish Parliament (Riksdag)</p> <ul style="list-style-type: none"> <li>• Mr A.H. VAN DELDEN, Chair of the Dutch independent Review Committee on the Intelligence and Security Services (CTIVD)</li> <li>• Ms Dorothee BELZ, Vice-President, Legal and Corporate Affairs Microsoft EMEA (Europe, Middle East and Africa)</li> <li>• Mr Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google</li> <li>• Mr Richard ALLAN, Director EMEA Public Policy, Facebook</li> </ul>
<p>14<sup>th</sup> November 2013 15.00 – 18.30 (BXL) <b>With AFET</b></p>	<p>- IT Security of EU institutions (Part I) (EP, COM (CERT-EU), (eu-LISA)</p> <p>- The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part III)(BE, DA)</p>	<ul style="list-style-type: none"> <li>• Mr Giancarlo VILELLA, Director General, DG ITEC, European Parliament</li> <li>• Mr Ronald PRINS, Director and co-founder of Fox-IT</li> <li>• Mr Freddy DEZEURE, head of task force CERT-EU, DG DIGIT, European Commission</li> <li>• Mr Luca ZAMPAGLIONE, Security Officer, eu-LISA</li> <li>• Mr Armand DE DECKER, Vice-Chair of the Belgian Senate, Member of the Monitoring Committee of the Intelligence Services Oversight Committee</li> <li>• Mr Guy RAPAILLE, Chair of the Intelligence Services Oversight Committee (Comité R)</li> <li>• Mr Karsten LAURITZEN, Member of the Legal Affairs Committee, Spokesperson for Legal Affairs – Danish Folketing</li> </ul>
<p>18<sup>th</sup> November 2013 19.00 – 21.30 (STR)</p>	<p>- Court cases and other complaints on national surveillance programs (Part II) (Polish NGO)</p>	<ul style="list-style-type: none"> <li>• Dr Adam BODNAR, Vice-President of the Board, Helsinki Foundation for Human Rights (Poland)</li> </ul>

2 <sup>nd</sup> December 2013 15.00 – 18.30 (BXL)	- The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part IV) (Norway)	<ul style="list-style-type: none"> <li>• Mr Michael TETZSCHNER, member of The Standing Committee on Scrutiny and Constitutional Affairs, Norway (Stortinget)</li> </ul>
5 <sup>th</sup> December 2013, 15.00 – 18.30 (BXL)	<p>- IT Security of EU institutions (Part II)</p> <p>- The impact of mass surveillance on confidentiality of lawyer-client relations</p>	<ul style="list-style-type: none"> <li>• Mr Olivier BURGERSDIJK, Head of Strategy, European Cybercrime Centre, EUROPOL</li> <li>• Prof. Udo HELMBRECHT, Executive Director of ENISA</li> <li>• Mr Florian WALTHER, Independent IT-Security consultant</li> <li>• Mr Jonathan GOLDSMITH, Secretary General, Council of Bars and Law Societies of Europe (CCBE)</li> </ul>
9 <sup>th</sup> December 2013 (STR)	<p>- Rebuilding Trust on EU-US Data flows</p> <p>- Council of Europe Resolution 1954 (2013) on ‘National security and access to information’</p>	<ul style="list-style-type: none"> <li>• Ms Viviane REDING, Vice President of the European Commission</li> <li>• Mr Arcadio DÍAZ TEJERA, Member of the Spanish Senate, - Member of the Parliamentary Assembly of the Council of Europe and Rapporteur on its Resolution 1954 (2013) on ‘National security and access to information’</li> </ul>
17 <sup>th</sup> -18 <sup>th</sup> December (BXL)	<p>Parliamentary Committee of Inquiry on Espionage of the Brazilian Senate (Videoconference)</p> <p>IT means of protecting privacy</p>	<ul style="list-style-type: none"> <li>• Ms Vanessa GRAZZIOTIN, Chair of the Parliamentary Committee of Inquiry on Espionage</li> <li>• Mr Ricardo DE REZENDE FERRAÇO, Rapporteur of the Parliamentary Committee of Inquiry on Espionage</li> <li>• Mr Bart PRENEEL, Professor in Computer Security and Industrial Cryptography in the University KU Leuven, Belgium</li> <li>• Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European</li> </ul>

	Exchange of views with the journalist having made public the facts (Part II) (Videoconference)	<p>Commission</p> <ul style="list-style-type: none"> <li>• Dr Christopher SOGHOIAN, Principal Technologist, Speech, Privacy &amp; Technology Project, American Civil Liberties Union</li> <li>• Christian HORCHERT, IT-Security Consultant, Germany</li> <li>• Mr Glenn GREENWALD, Author and columnist with a focus on national security and civil liberties, formerly of the Guardian</li> </ul>
22 January 2014 (BXL)	Exchange of views on the Russian communications interception practices (SORM)(via videoconference)	<ul style="list-style-type: none"> <li>• Mr Andrei Soldatov, investigative journalist, an editor of Agentura.ru</li> </ul>

## **ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS**

### **1. Experts who declined the LIBE Chair's Invitation**

#### **US**

- Mr Keith Alexander, General US Army, Director NSA<sup>55</sup>
- Mr Robert S. Litt, General Counsel, Office of the Director of National Intelligence<sup>56</sup>
- Mr Robert A. Wood, Chargé d'affaires, United States Representative to the European Union

#### **United Kingdom**

- Sir Iain Lobban, Director of the United Kingdom's Government Communications Headquarters (GCHQ)

#### **France**

- M. Bajolet, Directeur général de la Sécurité Extérieure, France
- M. Calvar, Directeur Central de la Sécurité Intérieure, France

#### **Germany**

- Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

#### **Netherlands**

- Mr Ronald Plasterk, Minister of the Interior and Kingdom Relations, the Netherlands
- Mr Ivo Opstelten, Minister of Security and Justice, the Netherlands

#### **Poland**

- Mr Dariusz Łuczak, Head of the Internal Security Agency of Poland
- Mr Maciej Hunia, Head of the Polish Foreign Intelligence Agency

#### **Private IT Companies**

- Tekedra N. Mawakana, Global Head of Public Policy and Deputy General Counsel,

---

<sup>55</sup> The Rapporteur met with Mr Alexander together with Chairman Brok and Senator Feinstein in Washington on 29<sup>th</sup> October 2013.

<sup>56</sup> The LIBE delegation met with Mr Litt in Washington on 29<sup>th</sup> October 2013.

Yahoo

- Dr Saskia Horsch, Senior Manager Public Policy, Amazon

#### **EU Telecommunication Companies**

- Ms Doutriaux, Orange
- Mr Larry Stone, President Group Public & Government Affairs British Telecom, UK
- Telekom, Germany
- Vodafone

#### **2. Experts who did not respond to the LIBE Chair's Invitation**

##### **Netherlands**

- Mr Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

##### **Sweden**

- Mr Ingvar Åkesson, National Defence Radio Establishment (Försvarets radioanstalt, FRA)

## RESULT OF FINAL VOTE IN COMMITTEE

<b>Date adopted</b>	12.2.2014
<b>Result of final vote</b>	+: 33 -: 7 0: 17
<b>Members present for the final vote</b>	Jan Philipp Albrecht, Roberta Angelilli, Mario Borghezio, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Agustín Díaz de Mera García Consuegra, Ioan Enciu, Frank Engel, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Salvatore Iacolino, Livia Járóka, Teresa Jiménez-Becerril Barrio, Timothy Kirkhope, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Louis Michel, Claude Moraes, Antigoni Papadopoulou, Georgios Papanikolaou, Judith Sargentini, Birgit Sippel, Csaba Sógor, Rui Tavares, Axel Voss, Tatjana Ždanoka, Auke Zijlstra
<b>Substitute(s) present for the final vote</b>	Alexander Alvaro, Anna Maria Corazza Bildt, Monika Hohlmeier, Stanimir Ilchev, Iliana Malinova Iotova, Jean Lambert, Marian-Jean Marinescu, Jan Mulder, Siiri Oviir, Salvador Sedó i Alabart
<b>Substitute(s) under Rule 187(2) present for the final vote</b>	Richard Ashworth, Phil Bennion, Françoise Castex, Jürgen Creutzmann, Christian Ehler, Knut Fleckenstein, Carmen Fraga Estévez, Nadja Hirsch, Maria Eleni Koppa, Evelyn Regner, Luis Yáñez-Barnuevo García, Gabriele Zimmer